NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(SAS-152)TP/1010

www.sto.nato.int

STO TECHNICAL REPORT **TR-SAS-152**

Conceptual Framework for Comprehensive National Defence System

(Cadre conceptuel d'un système national de défense complète)

Final report of Task Group SAS-152.

Published May 2024

NORTH ATLANTIC TREATY ORGANIZATION

SCIENCE AND TECHNOLOGY ORGANIZATION

AC/323(SAS-152)TP/1010

www.sto.nato.int

STO TECHNICAL REPORT **TR-SAS-152**

Conceptual Framework for Comprehensive National Defence System

(Cadre conceptuel d'un système national de défense complète)

Final report of Task Group SAS-152.

The NATO Science and Technology Organization

Science & Technology (S&T) in the NATO context is defined as the selective and rigorous generation and application of state-of-the-art, validated knowledge for defence and security purposes. S&T activities embrace scientific research, technology development, transition, application and field-testing, experimentation and a range of related scientific activities that include systems engineering, operational research and analysis, synthesis, integration and validation of knowledge derived through the scientific method.

In NATO, S&T is addressed using different business models, namely a collaborative business model where NATO provides a forum where NATO Nations and partner Nations elect to use their national resources to define, conduct and promote cooperative research and information exchange, and secondly an in-house delivery business model where S&T activities are conducted in a NATO dedicated executive body, having its own personnel, capabilities and infrastructure.

The mission of the NATO Science & Technology Organization (STO) is to help position the Nations' and NATO's S&T investments as a strategic enabler of the knowledge and technology advantage for the defence and security posture of NATO Nations and partner Nations, by conducting and promoting S&T activities that augment and leverage the capabilities and programmes of the Alliance, of the NATO Nations and the partner Nations, in support of NATO's objectives, and contributing to NATO's ability to enable and influence security and defence related capability development and threat mitigation in NATO Nations and partner Nations, in accordance with NATO policies.

The total spectrum of this collaborative effort is addressed by six Technical Panels who manage a wide range of scientific research activities, a Group specialising in modelling and simulation, plus a Committee dedicated to supporting the information management needs of the organization.

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These Panels and Group are the power-house of the collaborative model and are made up of national representatives as well as recognised world-class scientists, engineers and information specialists. In addition to providing critical technical oversight, they also provide a communication link to military users and other NATO bodies.

The scientific and technological work is carried out by Technical Teams, created under one or more of these eight bodies, for specific research activities which have a defined duration. These research activities can take a variety of forms, including Task Groups, Workshops, Symposia, Specialists' Meetings, Lecture Series and Technical Courses.

Published May 2024

ISBN 978-92-837-2330-1

Table of Contents

List of Figures

List of Tables

List of Acronyms

CBP	Capability-Based Planning
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CD	Comprehensive Defence
CDHQ	Comprehensive Defence Headquarters
CEO	Chief Executive Officer
CIS	Communication and Information Systems
CM	Crisis Management
COS	Chief of Staff
EDF	Estonian Defence Forces
EDL	Estonian Defence League
ENDDP	Estonian National Defence Development Plan
ENSC	Estonian National Security Strategy
FFI	Norwegian Defence Research Establishment
FNF	Fundamental National Function
GOV	Government of the Republic of Estonia
HQ	Headquarters
ICT	Information and Communication Technology
ISO	International Organization for Standardization
MEC	Ministry of Economy and Communications
MIA	Ministry of Internal Affairs
MOC	Ministry of Culture
MOD	Ministry of Defence
MOE	Ministry of Environment
MOF	Ministry of Finance
MOJ	Ministry of Justice and Public Security
MRA	Ministry of Rural Affairs
MSA	Ministry of Social Affairs
NAFv4	NATO Architecture Framework version 4
NATO	North Atlantic Treaty Organization
NCRS	NATO Crisis Response System
PoE	Parliament of Republic of Estonia
SOP	Standard Operating Procedure
SRA	Society for Risk Analysis
TRJE18	NATO Exercise Trident Juncture 2018

SAS-152 Membership List

CHAIR

Dr. Jaan MURUMETS
Estonian Military Academy
ESTONIA
Email: jaan.murumets@mil.ee

MEMBERS

Assoc.Prof. Erdal ARSLAN
Selcuk University
TURKEY
Email: erdalarslan@selcuk.edu.tr

Dr. Ieva BERZINA
Defence Academy of Latvia
LATVIA
Email: Ieva.Berzina@mil.lv

Dr Monica ENDREGARD
Norwegian Defence Research Establishment (FFI)
NORWAY
Email: Monica.Endregard@ffi.no

Col (Ret) Aarne ERMUS
Estonian Military Academy
ESTONIA
Email: Aarne.Ermus@mil.ee

Maj Andrew HOUSTON
DCDC, Defence Academy
UNITED KINGDOM
Email: Andrew.Houston208@mod.gov.uk

Maj Leenu ORG
Estonian Military Academy
ESTONIA
Email: leenu.org@mil.ee

MAJ Ivo PEETS
EDF HQ
ESTONIA
Email: Ivo.Peets@mil.ee

Mr. Aleksandr POPOV
Estonian Military Academy
ESTONIA
Email: aleksandr.popov@mil.ee

Capt Joaquim SOARES
Royal Military Academy
BELGIUM
Email: Joaquim.Soares@rma.ac.be

Prof. Dr. Sait YILMAZ
Esenyurt University
TURKEY
Email: saityilmaz@esenyurt.edu.tr

ADDITIONAL CONTRIBUTORS

Mr. William DEMEYERE
Control and Reporting Centre
BELGIUM
Email: william.demeyere@mil.be

LtCol. Dr. Geert LETENS
Royal Military Academy
BELGIUM
Email: geert.letens@gmail.com

Maj Maarten VERBURG
Belgian Defence HQ
BELGIUM
Email: Maarten.Verburg@mil.be

Conceptual Framework for Comprehensive National Defence System

(STO-TR-SAS-152)

Executive Summary

The main objective of this study is to research ways and means to coordinate and integrate activities of actors with different professional cultures, doctrines, tactics and techniques, and established practices. In terms of conceptual aspects of the comprehensive defence framework and application practices, the study aims to look at how different NATO members have approached the comprehensive defence framework, identifying the key actors and stakeholders.

The study has two phases. Phase 1 consisted of review of available literature on subject, and a series of case studies that largely follow the same uniform analytical approach. The aims of Phase 1 were twofold: first, to establish an empirical base – a snapshot of the existing perceptions, policies, rules and regulations, institutions, and procedures – potential use of which extends beyond the scope of this study. Second, to identify recurring themes and common shortfalls in the existing approaches.

The purpose of case studies was to describe Nations' approach to civil-military cooperation within the (evolving) framework of a Comprehensive National Defence Concept. In addition, to describe bi- and multi-lateral defence cooperation, or within an Alliance / Enhanced Partnership framework, and to ensure Nations are capable of coping with wide array of threats from natural and man-made disasters through hybrid threats to use of military force. For the purposes of National case studies, Comprehensive Defence is defined as situations involving the Military either in a lead or support role.

Throughout the case studies, several themes and topics emerged that challenge the further development and implementation of the comprehensive defence concept. Based on preliminary findings from case studies, selected aspects of the comprehensive defence concept were further addressed in multiple domains from multiple angles whilst using intellectual tools from multiple scientific disciplines.

Part 2 begins with two different perspectives of conceptual underpinnings of comprehensive defence approach. These include addressing the challenges of managing relations and expectations between society and defence, and looking at the cognitive dimension of comprehensive national defence. The following two chapters deal with systemic approaches to the concept, elaborating on the risk-based approach to national security, and exploring the applicability of enterprise architecture and capability-based planning methodologies to comprehensive defence. Further, the comprehensive defence concept is elaborated in the context of city security, followed by a look at legal aspects of integrating Armed Forces into internal security tasks. A concept model for combined comprehensive defence headquarters is presented in the penultimate chapter. Finally, the problem of the adaptation of emerging technologies for defence is addressed.

Over the next few years, this rapidly evolving body of observations, analyses and recommendations will provide an extensive basis from which to substantively re-examine the assumptions, key parameters, and expected outcomes of the implementation of the concept of comprehensive defence. Hence, this report should be seen as an early stepping-stone in a long process of development and practical application of the comprehensive defence concept.

Cadre conceptuel d'un système national de défense complète

(STO-TR-SAS-152)

Synthèse

L'objectif principal de la présente étude est de rechercher les moyens de coordonner et intégrer les activités des acteurs ayant différentes cultures professionnelles, doctrines, tactiques, techniques et pratiques établies. Sur le plan des aspects conceptuels du cadre de défense complète et des pratiques d'application, l'étude vise à examiner comment les différents membres de l'OTAN ont abordé le cadre de défense complète et qui sont les acteurs et parties prenantes clés.

L'étude s'est articulée en deux phases. La première phase a consisté en une revue de la littérature disponible sur le sujet et une série d'études de cas qui suivaient largement une démarche analytique uniforme. Les objectifs de la première phase étaient doubles : premièrement, établir une base empirique – un instantané des perceptions, politiques, règles et réglementations, institutions et procédures existantes – dont l'utilisation potentielle s'étend au-delà du champ d'application de cette étude ; deuxièmement, identifier les thèmes récurrents et les lacunes courantes des approches existantes.

L'objet des études de cas était de décrire l'approche d'un pays en matière de coopération civilo-militaire dans le cadre (en constante évolution) du concept de défense nationale complète. Il s'agissait également de décrire la coopération bilatérale et multilatérale dans le domaine de la défense, ou au sein d'une alliance/d'un partenariat renforcé, et de s'assurer que le pays était capable de faire face à un large éventail de menaces, allant des catastrophes naturelles et d'origine humaine jusqu'aux menaces hybrides, en passant par l'utilisation de la force militaire. Aux fins des études de cas nationales, la défense complète est définie comme une situation qui implique l'armée, dans un rôle prépondérant ou de soutien.

Les études de cas ont fait émerger plusieurs thèmes et sujets qui remettent en question le développement ultérieur et la mise en œuvre du concept de défense complète. Sur la base des conclusions préliminaires des études de cas, certains aspects du concept de défense complète ont été traités plus en détail dans de multiples domaines et sous plusieurs angles, à l'aide d'outils intellectuels issus de multiples disciplines scientifiques.

La deuxième partie commence par deux perspectives différentes sur les fondements conceptuels de la défense complète. L'une consiste à s'occuper de la gestion des relations et des attentes entre la société et la défense et l'autre, à examiner la dimension cognitive de la défense nationale complète. Les deux chapitres suivants traitent des approches systémiques du concept. Ils développent l'approche de la sûreté nationale basée sur les risques et étudient la possibilité d'appliquer à la défense complète l'architecture d'entreprise et les méthodologies de planification basées sur les capacités. Ensuite, le concept de défense complète est traité en détail dans le contexte de la sûreté urbaine, puis les aspects juridiques de l'intégration des forces armées dans les tâches de sûreté intérieure sont examinés et l'avant-dernier chapitre présente un modèle de concept pour les états-majors combinés de la défense complète. Enfin, on aborde la problématique de l'adaptation des technologies émergentes à la défense.

L’évolution rapide du corpus d’observations, analyses et recommandations fournira au cours des prochaines années une base étendue pour réexaminer en substance les hypothèses, les paramètres clés et les résultats attendus de la mise en œuvre du concept de défense complète. Par conséquent, le présent rapport doit être considéré comme la première étape d’un long processus de développement et d’application pratique du concept de défense complète.

Chapter 1 – INTRODUCTION

Jaan Murumets, SAS-152 Chair
Estonian Military Academy
ESTONIA

1.1 CONTEXT AND PURPOSE

In an ever-changing security environment, military and civil institutions need to cooperate. Operational experience has taught us that military means, although essential, are not enough on their own to meet the many complex challenges to security. The military must work with other actors to contribute to a comprehensive approach that effectively combines political, civilian, and military crisis management instruments. Its effective implementation requires all actors to contribute in a concerted effort, based on a shared sense of responsibility, openness, and determination, and taking into account their respective strengths, mandates and roles, as well as their decision-making autonomy. Operating in such a way creates enhanced resilience and contributes to shared political-military situational awareness in line with the new NATO Strategic Concept of 2022.

Information sharing and mutually understandable operating procedures are the prerequisites for comprehensive defence, aligning objectives, structures, processes and procedures amongst diverse stakeholders and contingencies.

As various models of comprehensive defence are implemented in different NATO member and Partner states, there is a need to study the conceptual underpinnings, as well as methods for planning, analysing, and validating the capability requirements and concepts of operation. For the purposes of this study, the national comprehensive defence system is broadly understood as coordinated cooperation of different government, public, private, and non-governmental organisations with military structures, integrating different operating concepts, methods of Command and Control, information flows, and processes and procedures.

Planning for, and conduct of operations in a complex, multi-domain environment with involvement of different military, paramilitary, and non-military organisations, to include countering hybrid threats, requires a coherent conceptual framework to ensure shared understanding of missions, tasks, capability requirements, and concepts of operation. Civilian resources and capabilities as enablers to military operations (e.g., strategic lift) have gained increasing importance. In addition, the ability to support allies and partners with non-military capabilities can free up resources for additional military capabilities.

This study is strongly linked to the ongoing research taking place in countries represented at the Research Task Group (RTG) by addressing aspects of the concept of Comprehensive Defence similar to or compatible with those examined in home nations, and carried out partially by the members of the RTG. Prime examples of such synergy are research ongoing in Belgium on Performance Management in a multi-stakeholder context, research ongoing in Estonia on the development of a National-level system for Situation Awareness, research ongoing in Norway on further development of the Comprehensive Defence concept and its implementation, and research ongoing in Latvia on the initial implementation of the Comprehensive Defence concept.

1.2 STRUCTURE OF THE REPORT

This report combines two sets of contributions. The first part of the volume is comprised of outlines of the study provided in this introductory chapter, followed by separate chapters – Chapters 2 through 9 – of review of available literature on the topic of comprehensive defence, and case studies arranged in alphabetical order of subject Nations. The results of Phase 1 – in the form of an interim report – were pre-released by NATO

STO in January 2021. Chapters 10 to 17 address in-depth some of the topics identified in the National case studies. The sequence of these chapters has been discussed and agreed by the working group and reflects the broader logic of the comprehensive defence concept. Finally, preliminary findings from case studies, identified challenges, and a list of topics to be further researched as well as highlights of topical studies are provided in Chapter 18. All the Phase 2 work took place from early 2021 through June 2022.

In order to keep referencing understandable and manageable, the working group agreed that references to source documents are provided separately at the end of each chapter.

1.3 DESIGN OF THE STUDY

1.3.1 Overall Outlines

The main objective of this study is to research ways and means to coordinate and integrate activities of actors with different professional cultures, doctrines, tactics and techniques, and established practices. In terms of conceptual aspects of the comprehensive defence framework and application practices the study aims to look at how have different NATO members approached the comprehensive defence framework, identifying key actors and stakeholders. The identification of benefit and limitations of comprehensive defence frameworks and discussion of future perspectives of international collaboration on comprehensive defence also falls squarely into the broader scope of this study.

The study has two phases. Phase 1 consists of a review of available literature on subject, and a series of case studies that largely follow the same uniform analytical approach. The aims of Phase 1 are twofold: first, to establish an empirical base – a snapshot of the existing perceptions, policies, rules and regulations, institutions, and procedures – potential use of which extends beyond the scope of this study. Second, to identify recurring themes and common shortfalls in the existing approaches some of which are explored in-depth in Phase 2 of the study.

Phase 2, in turn, aims to elaborate on select aspects of the comprehensive defence concept in multiple domains and from multiple angles whilst using intellectual tools from multiple scientific disciplines. The focus and scope of individual chapters varies from high-level conceptual discussions to practical applications of facets of the concept. The selection of topics for studies within Phase 2 reflects the main areas of study of the working group members rather than an attempt to exhaustively cover all the facets of the underlying concept of comprehensive defence.

1.3.2 Analytical Architecture for National Case Studies

The purpose of the case studies is to describe the Nations' approach to civil-military cooperation within the (evolving) framework of Comprehensive National Defence Concept. In addition, to describe bi- and multi-lateral defence cooperation, or within an Alliance / Enhanced Partnership framework, and to ensure Nation is capable of coping with wide array of threats from natural and man-made disasters through hybrid threats to use of military force. For the purposes of National case studies, Comprehensive Defence is defined as situations involving the Military either in lead or support role.

Specific topics to be addressed within each case study encompass:

- Threat perception, national objectives, and priorities. That means primarily references to national strategy documents, e.g., parliamentary endorsed National Security Strategy, Long-term National Defence Development Plan, or quadrennial Public Security Report to Parliament.
- Relevant references to the concept of Comprehensive Defence in National strategic documents. This would include the scope of situations that would prompt the military involvement and may differ a lot between countries.

- Internal and international Command and Control and logistical interoperability. Within this broad category, development of closer insights into specific areas:
  - Available doctrinal framework and possible gaps in it. Sources for this analysis would include, e.g., agreement between MOD and Police on joint training, or government policy on joint procurement of small arms for the Armed Forces and Law Enforcement Agencies.
  - Organisational setup related to civil-military crisis management, to include provisions for receiving and providing international support. Sources for this analysis would include, e.g., standing crisis management legislation, permanent or ad hoc coordinating structures (anti-terrorism, maritime functions).
  - Roles, responsibilities, authorities, and technical competency of different stakeholders.
  - Standing legal provisions for activation of the system and further escalation. Circumstances and mechanisms by which agencies start working together, to include international cooperation.
- Challenges of implementation. Within this broad category, development of closer insights into specific areas:
  - Role of organisational culture and institutional barriers (to include budgets) in enabling or disabling cross-agency cooperation.
  - Joint planning, training, and procurement.
  - Compatibility and interoperability of Standing Operating Procedures and equipment across multiple stakeholder agencies.
  - Societal perceptions and support. This would address expectations to the public (e.g., being self-sufficient for 72 hours), civil defence awareness and related education and training at schools or businesses, public support to civil defence measures, and popular "will to defend" the country.
- Future developments and ongoing discussions.
- Preliminary conclusions.

1.3.3 Outlines of Part 2

At the end of Phase 1, the working group identified a handful of broad topics that challenge the further development and implementation of the comprehensive defence concept. Within that emerging framework of challenges and topics of interest, Part 2 of this report begins with two different perspectives of conceptual underpinnings of comprehensive defence approach. Those include addressing the challenges of managing relations and expectations between society and defence, and looking at the cognitive dimension of comprehensive national defence. The following two chapters deal with systemic approaches to the concept, elaborating on the risk-based approach to national security, and exploring applicability of enterprise architecture and capability-based planning methodologies onto comprehensive defence. Further, the comprehensive defence concept is elaborated in the context of city security, followed by a look at the legal aspects of integrating Armed Forces into internal security tasks, and presenting a concept model for combined comprehensive defence headquarters in the penultimate chapter. Finally, the problem of adapting emerging technologies for defence is addressed.

1.4 CHALLENGES TO THE WORK

It should be underscored that different Nations have adopted different approaches to the concept of Comprehensive Defence, and have different accumulated experience – some Nations for decades, while some are just in early stages of exploring the concept. Therefore, the analytical construct described in Section 1.3.2 above provides the backbone for a case study but depending on the availability of information, not every facet of the analytical construct is addressed in every case study.

The outbreak of COVID-19 severely influenced the execution of the SAS-152 plan of work. The original plan envisaged workshops together with invited external experts to present, discuss and refine case studies. The travel bans and cancellation of physical meetings within NATO and most of member states made these workshops impossible to conduct. The substitute for physical workshops SAS-152 working group ended up using was peer review of each case study by another working group member.

The COVID-19 outbreak also changed somewhat the focus of case studies. After deliberations, the working group decided not to write separate, COVID-dedicated sub-chapters but to address the pandemic within the agreed analytical framework when and where appropriate. However, COVID-related observations and findings from national case studies are compiled into a dedicated paragraph in the Chapter 18.

Another external factor that shaped the work of the research task group was Russian aggression against Ukraine. The research conducted by working group members under the guidance of their home organisations separate from this study, combined with emerging empirical data up to date, has underscored the potential of comprehensive defence concept to counter the onslaught of a quantitatively – though not necessarily qualitatively – superior adversary. At the time of finalising this report in summer of 2022, the available open source literature about the war is extremely limited and thus cannot be used to substantially inform Phase 2, although when and where appropriate, the preliminary observations related to the Ukraine war have been integrated into study chapters.

As was the case with the Phase 1, travel restrictions because of COVID-19 confined the working group interactions mainly to virtual meetings. As a result, when finalising and putting together the Phase 2 studies, the SAS-152 working group had to revert to the same process as was used for the Phase 1. Each chapter in Phase 2 compendium was therefore peer-reviewed by other working group members during the virtual meetings. The original study design envisaged thorough discussions in a workshop format for both Phases 1 and 2.

Finally, it is clear that this rapidly evolving body of observations, analyses and recommendations will provide over the next few years an extensive basis from which to substantively re-examine the assumptions, key parameters and expected outcomes of the implementation of the concept of comprehensive defence. Hence, this report should be seen as an early stepping-stone in a long process of development and practical application of the comprehensive defence concept.

Chapter 2 – A LITERATURE REVIEW ON COMPREHENSIVE NATIONAL DEFENCE SYSTEMS

Joaquim Soares
Royal Military Academy
BELGIUM

2.1 INTRODUCTION

Since the end of the Cold War and the terrorist attacks of 11 September 2001, the strategic context has been changing very rapidly. Where there used to be a hostile but stable environment, today's security environment is characterised by a high degree of complexity and asymmetry. This complexity manifests itself within several areas and situations including failed states, regional insecurity, hybrid warfare and global terrorism [15]. Deterring these threats and managing these challenges requires enhanced resilience, is subject to deploying means not limited to the military and necessitates coordination with different stakeholders at various policy levels. Not only global challenges, but also national problems such as declining defence budgets require defence organisations to evolve from a traditional and pure military focus [17]. Therefore, concepts such as comprehensive defence which bring together a large number of stakeholders around a holistic approach have become increasingly important and require further development [55]. Whereas different nuances, approaches and definitions exist such as Comprehensive Approach (CA), whole-of-government, whole-of-society, Defence, Development, and Diplomacy (3D), Total Defence etc., the focus of this study is to provide an overview that characterises the overall research area. For the purpose of simplicity, the concept in its generic meaning is further referred to as CA.

Given the importance of the research area and its quick development, NATO constituted a Research Task Group (RTG) called SAS-152 within which willing nations could share information on the status of their comprehensive defence initiatives. Within the RTG, data from seven countries is being collected, primarily through detailed national case studies. Besides these case studies and given the presumed diversity and complexity of the research area, a literature review was deemed necessary to provide a suitable introduction, summary, and overview prior to the comparison of national CA-related initiatives. A Systematic Literature Review (SLR) was therefore conducted focussing on CA within defence organisations which is the focus of this report. The results of the SLR include a core set of papers supplemented by documents from national Subject Matter Experts (SME). Besides being the first SLR identified in the field of CA, our study provides a conceptual and strategic platform for the SME's to further engage on the subject and to compare their respective national approaches. It also includes the most commonly identified challenges and some good practices for managers. Thereby, this study contributes towards the further development of the CA concept within defence organisations.

Having introduced the research area and the study scope, the remainder of the chapter is structured as follows. First, the research objective and the research questions are clarified. This is followed by a presentation of the methodology used to generate the answers to the research questions. Thereafter the main bibliographic and other findings of the study are presented. A discussion section then follows including insights and managerial implications. The chapter ends with a conclusion, the principal study limitations, and some avenues for further research. The final paper set is presented in Appendix 2-1.

2.2 RESEARCH OBJECTIVE AND RESEARCH QUESTIONS

As previously stated, our intent is not to dwell upon the exact doctrinal definition, terminology, and nuances of all CA-related concepts, but rather to provide an overview of the characteristics of the research area. Our first research question is therefore: What are the bibliometrics that characterise the research area?

As it appears that a CA and its related concepts imply collaboration between a variety of stakeholders that influence or are influenced by a defence organisation, it appears important to identify, describe and classify these stakeholders. This is because analysing, taking into account, and meeting expectations is critically important for the functioning of the organisation [9]. As the relationships with these stakeholders and their expectations change over time, it is also equally important to constantly keep track of stakeholder developments [47]. Identifying stakeholders and linking them with some of the previously mentioned CA concepts should enlighten us as to the approaches used and their comprehensiveness within various countries. Our second research question is therefore: Who are the main actors and stakeholders that are part of CA-related approaches and frameworks?

Our third research objective is to further study the various approaches and frameworks that are found in the literature. In doing so, and in combination with the two previous objectives, a suitable platform is provided for discussing the benefits and limitations of national initiatives. Our third research question is therefore: What are the benefits and limitations of the different comprehensive defence frameworks?

2.3 METHODOLOGY

In pursuance of answers towards our research questions, we performed a Systematic Literature Review (SLR) to investigate the status quo of CA in the literature. For the SLR, we used the overall six-step process modified from Higgins et al., [21] and Tranfield et al., [48] consisting of problem definition (phase one), scoping study (phase two), search strategy (phase three), exclusion criteria (phase four), data collection (phase five) and synthesis (phase six) as indicated in Figure 2-1.

Phase one (problem definition) was based on the research objectives and questions determined during RTG discussions. As discussions indicated a lot of diversity and complexity within the research area, a broad scoping study was conducted in phase two to include a wide range of disciplines (such as military, security, strategic communication, diplomacy, stakeholders' management…) and perspectives (such as war, peace, and armed conflict). Ultimately, the scoping set was chosen to address the research questions, to reflect the field diversity, and allow capture rate testing in phase three.

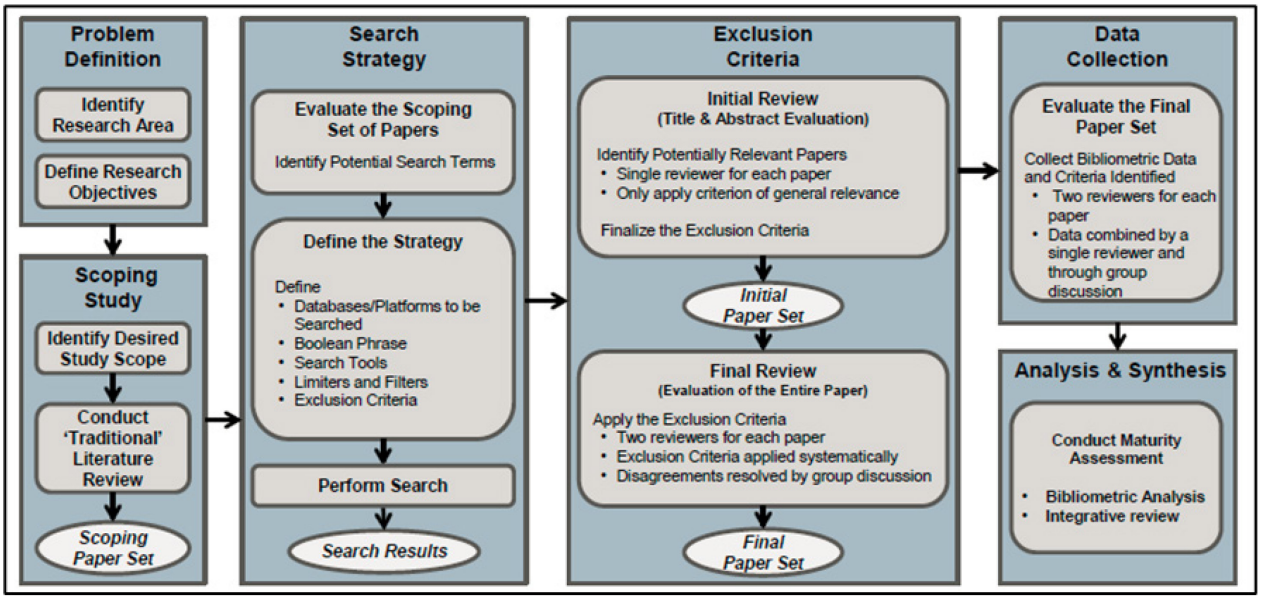

Figure 2-1: SLR Process Adapted from Higgins et al., [21] and Tranfield et al., [48].

In phase three, the scoping set papers were evaluated as well as the potential search terms. Keywords from the Technical Activity Proposal (TAP) were also included. In total, four researchers conducted several rounds of brainstorming on the keywords in order to select those terms that would be tested and ultimately make up the Boolean phrase. This Boolean phrase consisted of four categories of terms that were connected by Boolean operators as shown in Formula 2-1 below:

$$\text{CATEGORY 1 AND (CATEGORY 2 OR CATEGORY 3) AND CATEGORY 4} \quad (2\text{-}1)$$

CATEGORY 1 included terminology related to the military such as “defence” or “army”. Next, CATEGORY 2 included information pertaining to stakeholders such as “partner” and “actor”. CATEGORY 3 then contained terminology pertaining to the comprehensive approach itself such as “comprehensive” and “interagency”. Finally, CATEGORY 4 consisted of a list of terms that one may expect to encounter along with the first three categories such as “policy” and “strategy”. All the retained keywords (and identified variants, including all the TAP keywords) were tested during this phase based on the relevancy of the search results and the capture rate.

In doing so, insights from the previous phases influenced the search strategy. First, it was deemed necessary to obtain a mix of peer-reviewed and practitioner documents and it was accordingly decided to search both academic and professional platforms. Scopus was selected as the academic platform as it provides extensive, quality and consistent coverage around the globe [4], [20] and was readily available to the researchers via their institutions. The NATO library and the national defence library (called SharePoint) were selected for professional literature for some of the same reasons. Second, initially, as few limiters as possible were placed. This included the language that had to be either English, French or Dutch as these were the languages commonly understood amongst the researchers. Additionally, books, book chapters and newspaper type publications were excluded due to the lack of a peer review process, the difficulty for subsequent data collection and due to a general lack in guaranteed quality. Next, we also constrained the search as from 2005 to prioritise modern developments in the fields as it appeared that 9/11 (2001) and the Iraq War (2003) may have had an important impact [14], [27], [29]. Further, we carefully excluded some non-relevant domains such as agriculture and mathematics. Finally, we specifically excluded results containing a certain word using the NOT operator such as results containing the terms “suicide” and “religion”. The search was then executed based on title, keywords and abstract in Scopus and an equivalent technique on the other two platforms. Given the broad search strategy and categories, we identified 10121 unique results in Scopus and 1051 unique results in the NATO library while it was not possible to generate the exact number in SharePoint as depicted in Table 2-1.

Table 2-1: Initial Search Results per Platform (N).

Database	Limited Results	Initial Review	Second Review
Scopus	10 121	783 (631 available)	129
SharePoint	/	84	11
NATO Library	1051	23 (+43 doubles with Scopus)	7

The following tables and figures contain some of the other results of phase three from the Scopus platform.

From Figure 2-2, we can observe a constant increase in the number of publications over the years. This trend is not affected by the 2005 limitation. Note that in the figure data from the year 2020 has been voluntarily suppressed.

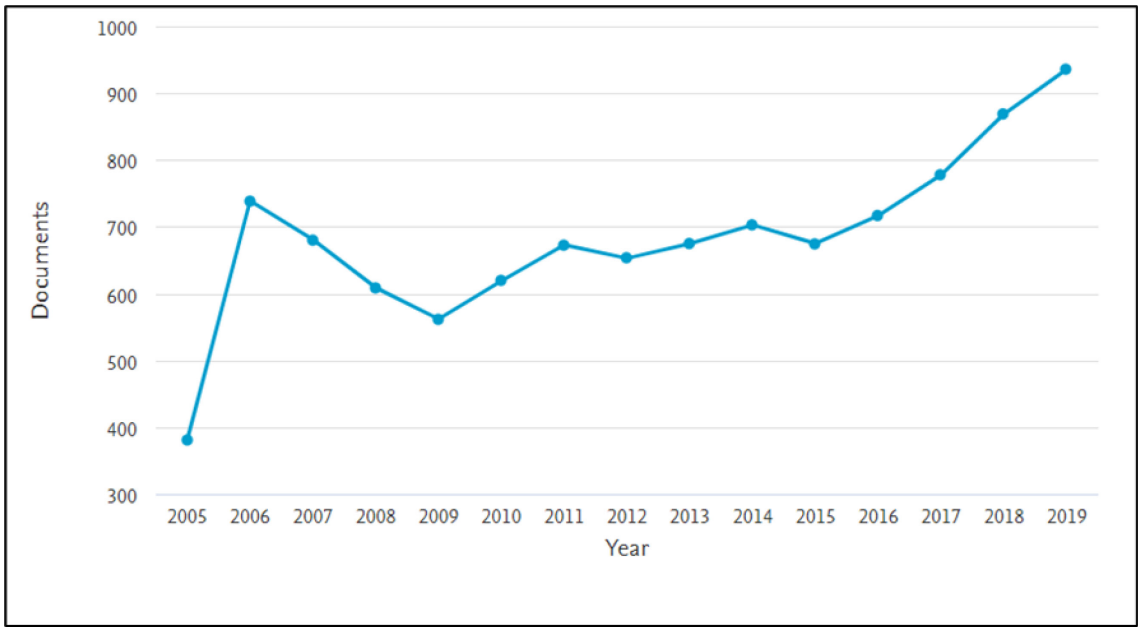

Figure 2-2: Number of Documents per Year Initial Results (Scopus).

From Figure 2-3, combined with our search strategy and choice of platforms, we may infer that we may be under sampling conference-type publications (which are none the less 18 percent of Scopus results) as they tend to be published on alternative platforms such as ProQuest or Ebscohost.

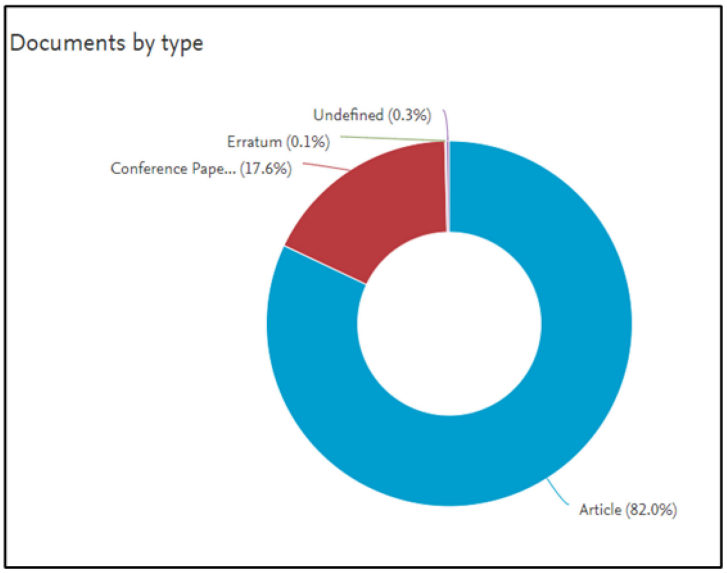

Figure 2-3: Type of Documents per Year Initial Results (Scopus).

When considering Figure 2-4, Figure 2-5, and Figure 2-6 together, the subject areas of the top ten journals from this phase indicate a large diversity in the field. As such, it may seem that researchers wanting to publish on this topic may want to consider a journal such as International Affairs based on the journal ranking and the number of previously published articles on the topic.

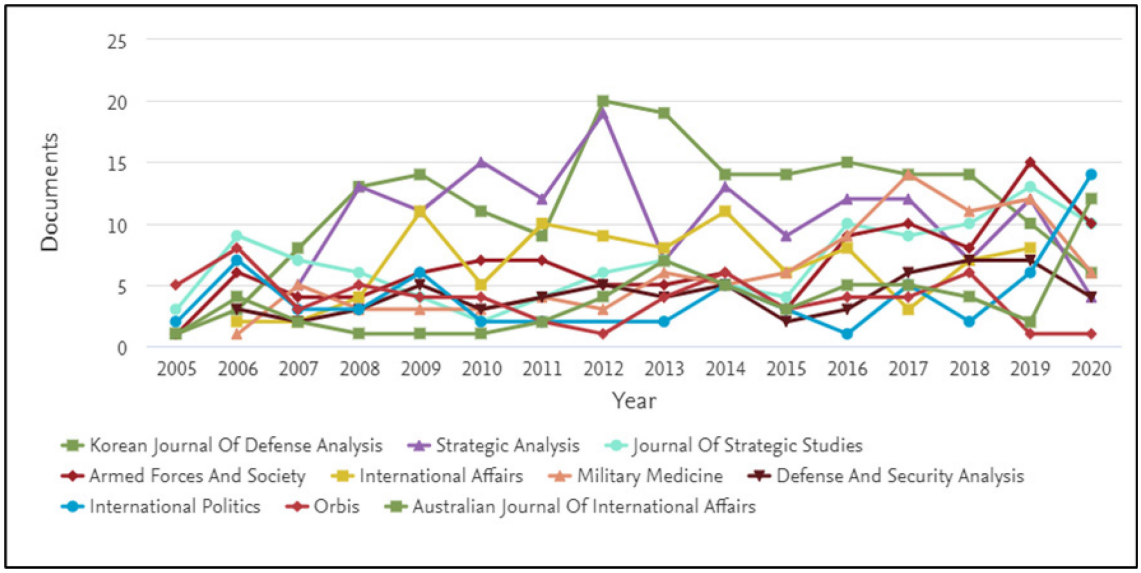

Figure 2-4: Number of Documents Published per Year in the Top 10 Journals Initial Results (Scopus).

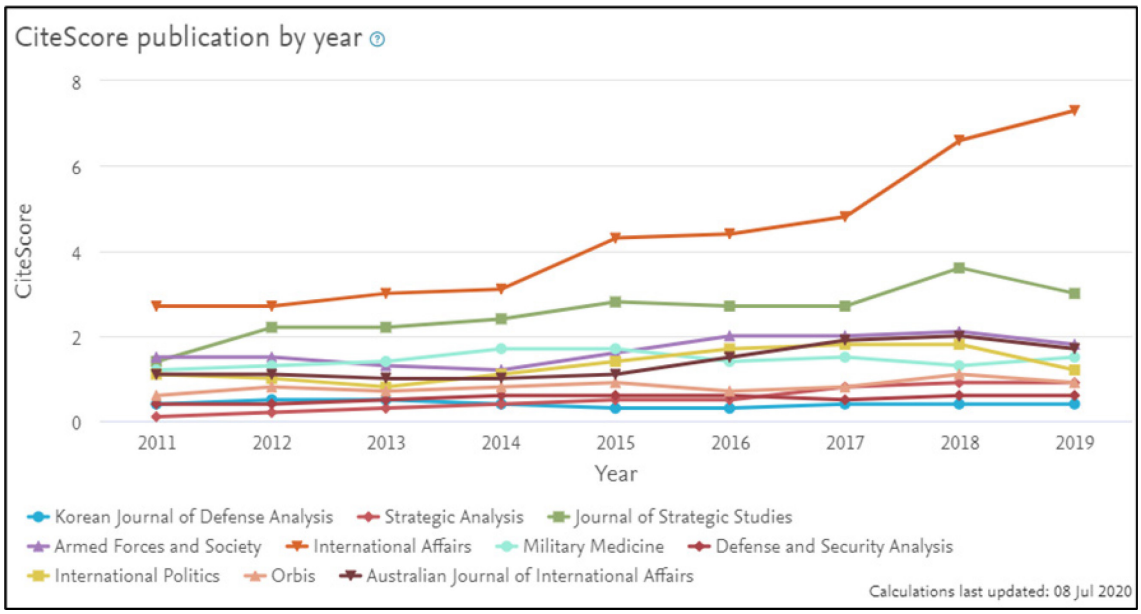

Figure 2-5: CiteScore per Year of the Top 10 Journals Initial Results (Scopus).

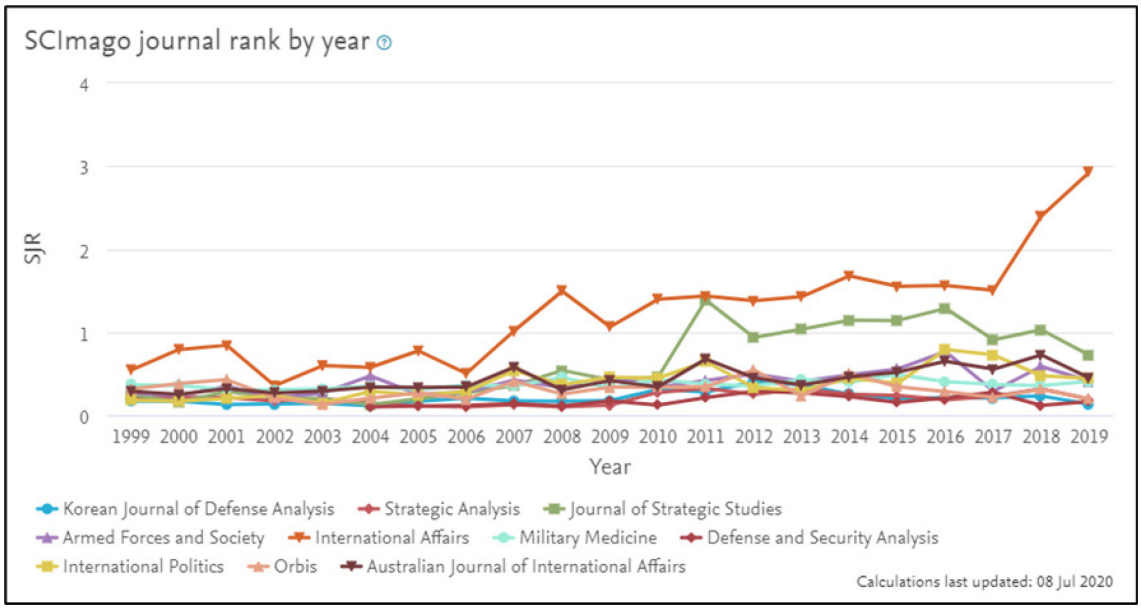

Figure 2-6: SCImago Journal Rank per Year of the top 10 Journals Initial Results (Scopus).

At first look at Figure 2-7, it appears that the top ten authors have 19 or more publications post 2005 with the top author having 75 publications indexed in Scopus. Researchers wanting to identify experts for symposiums or consulting purposes may want to have a closer look at the exact nature of publications of these different authors however given the previously indicated field diversity.

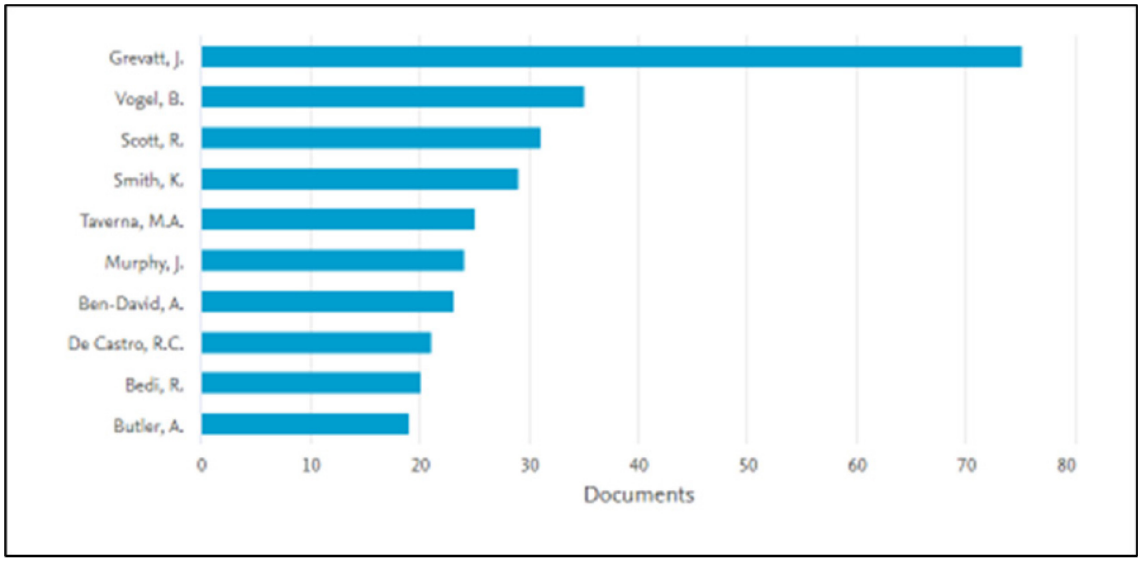

Figure 2-7: Number of Documents per Top Ten Authors Initial Results (Scopus).

When considering Figure 2-8, one can infer that the majority of countries being studied are NATO countries with the USA and the UK largely ahead even if there are significant amounts of publications from some other powerful countries such as China and India or countries facing significant military threats such as India and South Korea.

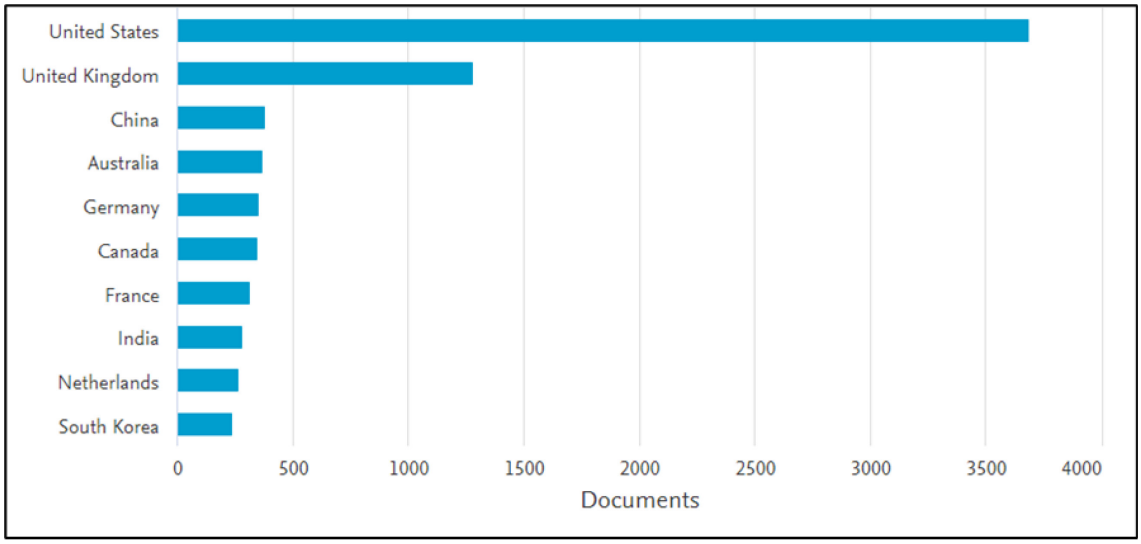

Figure 2-8: Number of Documents per Top Ten Countries Initial Results (Scopus).

When considering Figure 2-9, which is the same as the previous figure but only incorporates the data for NATO and EU countries, indications are that some of the likely most mature countries in the field such as the USA may not be represented in the RTG even if this will have to be confirmed in the final results.

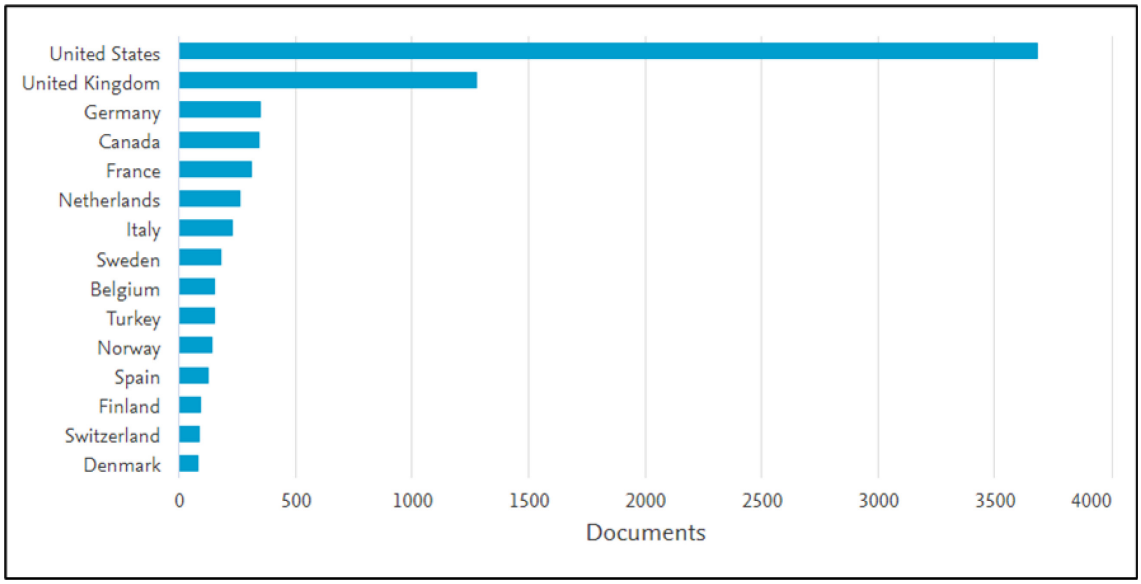

Figure 2-9: Number of Documents per Top Fifteen NATO and EU Countries* Initial Results (Scopus, *including Switzerland).

Finally, Figure 2-10 reconfirms the diversity of the research topic as characterised by the different subject areas recorded in Scopus. This tool may not be the most adequate however given the lack of clarity on how Scopus records the subject areas and an alternative assessment using specific bibliometric software or qualitative analysis may be required to better analyse the results.

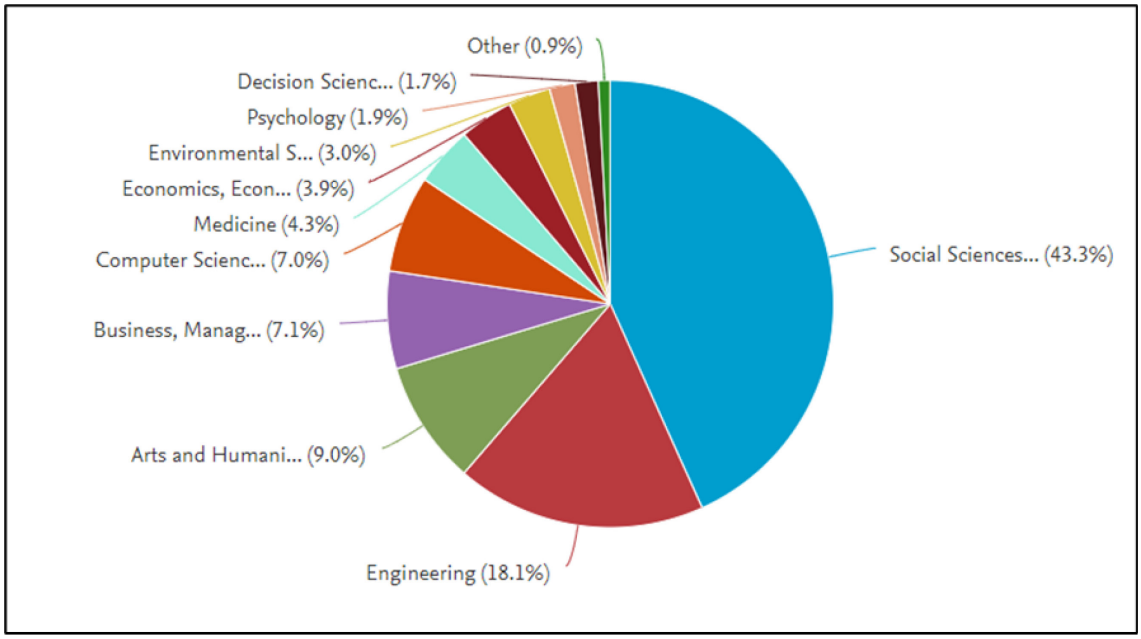

Figure 2-10: Catalogued Research Domains for the Initial Results (Scopus).

In phase four, we conducted the initial review based on the title and abstract of each paper to identify the results that were relevant or potentially relevant. In case of doubt about the relevancy, papers were preserved for the second review of phase five. In Scopus, out of the 783 papers identified, 631 were made available through open access, Google Scholar, researcher institution or through specific requests via the researcher's network. Out of the 152 documents that could not be accessed, 6 articles could only be found in Spanish or Turkish, 69 articles were publications from Jane's Defence that were possibly wrongly categorised in Scopus and 77 documents were simply not open access or retrievable. For completeness, a sample of 21 Jane's Defence publications were examined and deemed not to meet the exclusion criteria. A similar process led to the selection of 23 papers on the NATO platform (43 were duplicates previously identified in Scopus) and 85 results in SharePoint (none of which were duplicates). Since the documents in SharePoint did not contain an abstract, the initial review was conducted based on the keywords, title, the research domain, and the introduction.

The following tables and figures depict results of phase four from the Scopus platform.

From Figure 2-11, it appears that we retained a relatively constant number of papers up to 2017 – 2018 after which our retention rate increased significantly. Note that in the figure data from the year 2020 has been voluntary suppressed.

From Figure 2-12, and in comparison with Figure 2-3, we may infer that we retained journal articles at a higher rate than conference papers during this phase.

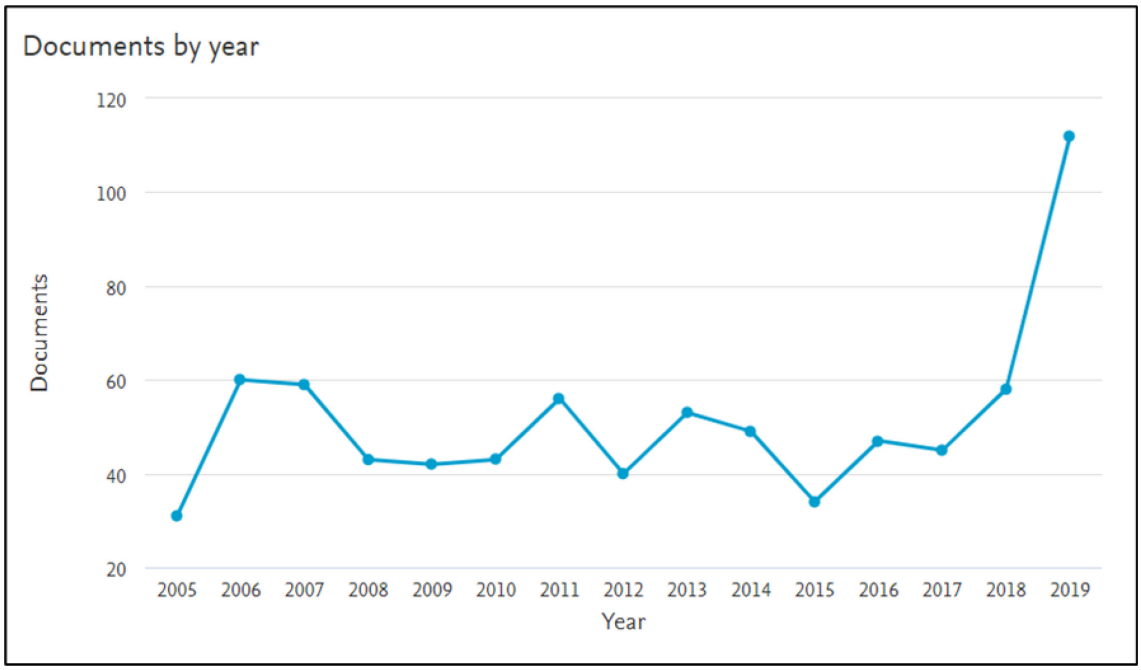

Figure 2-11: Number of Retained Documents per Year in Phase Four (Scopus).

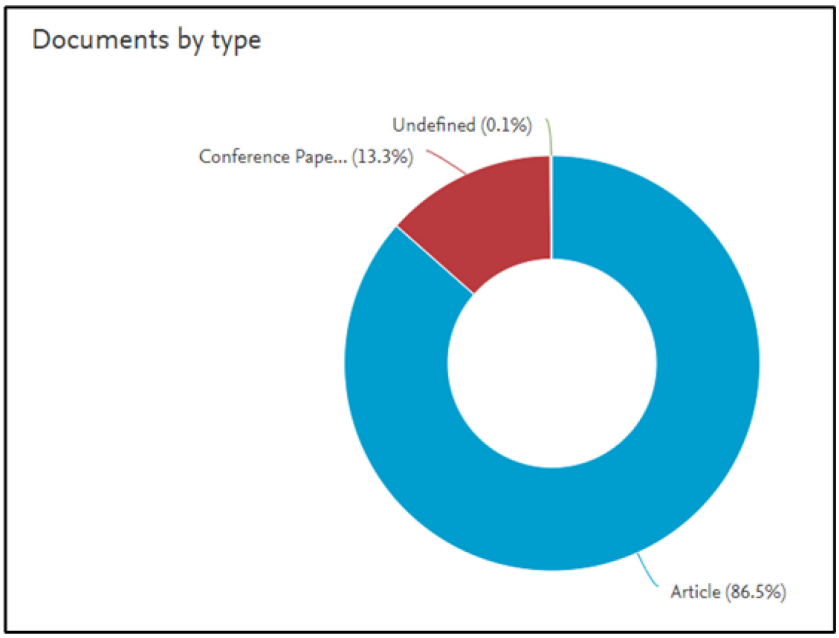

Figure 2-12: Types of Retained Documents in Phase Four (Scopus).

When comparing Figure 2-13 and Figure 2-4, we find that the documents retained originate from some of the same journals previously reported even if there are changes in the ranking. As such, Strategic Analysis, International Politics, Orbis and the Australian Journal of International Affairs are now replaced by International Peacekeeping, Contemporary Security Policy, Defence Studies and Disaster Medicine and Public Health Preparedness in the top ten.

Similarly to Figure 2-4, Figure 2-5, and Figure 2-6; Figure 2-13, Figure 2-14 and Figure 2-15 also indicate that, at this point, International Affairs may be the most coveted journal for publication on the research topic.

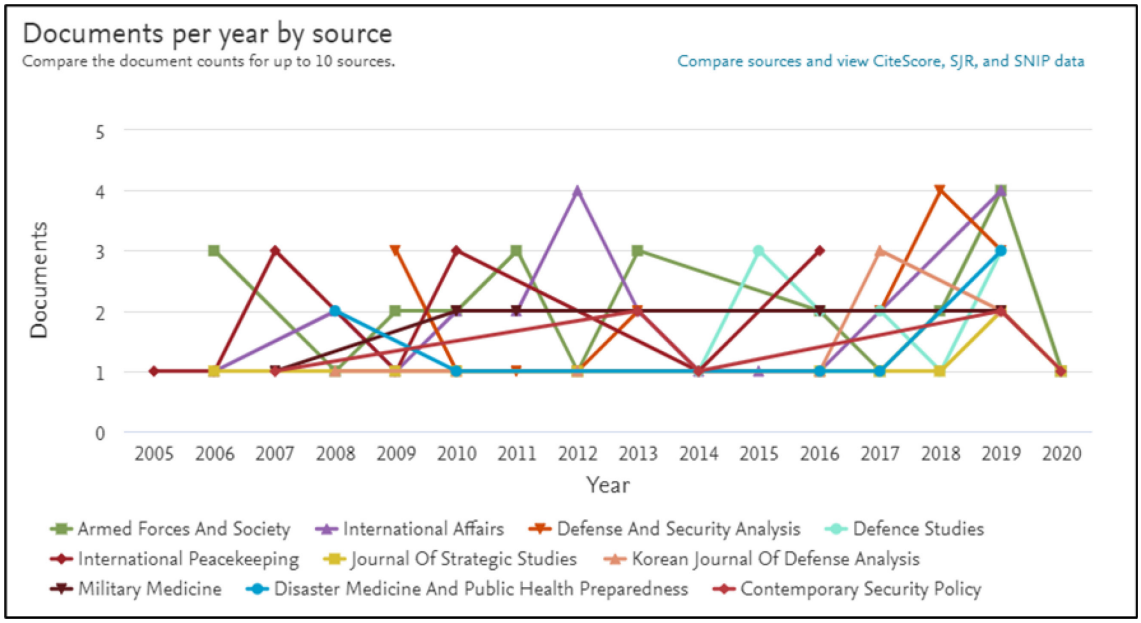

Figure 2-13: Number of Retained Documents in Phase Four Published per Year in the Top Ten Journals (Scopus).

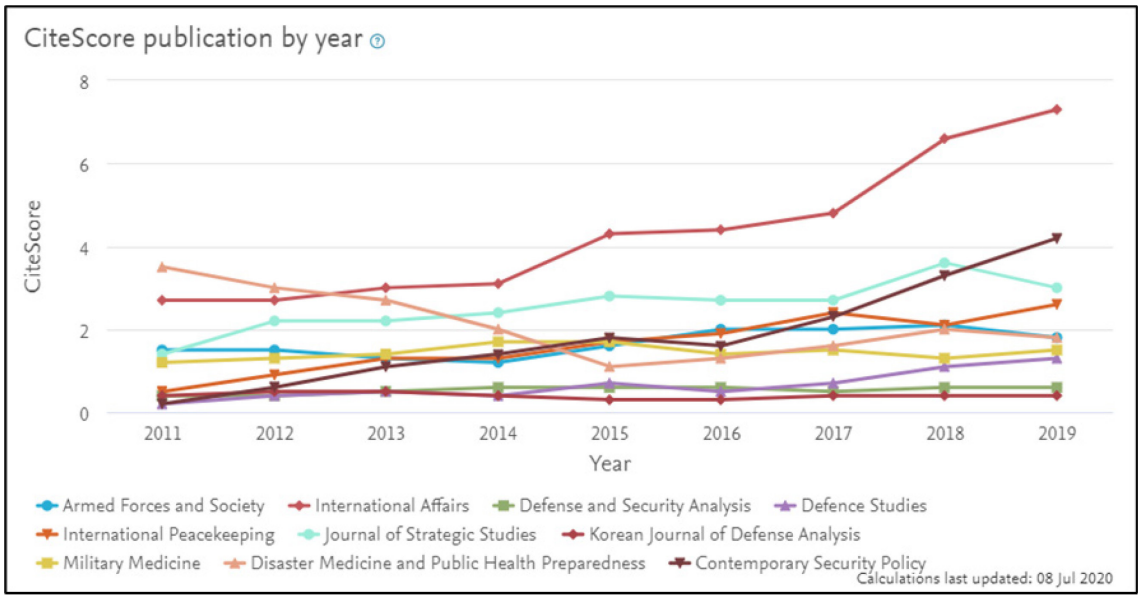

Figure 2-14: CiteScore per Year of the Top Ten Journals in Phase Four (Scopus).

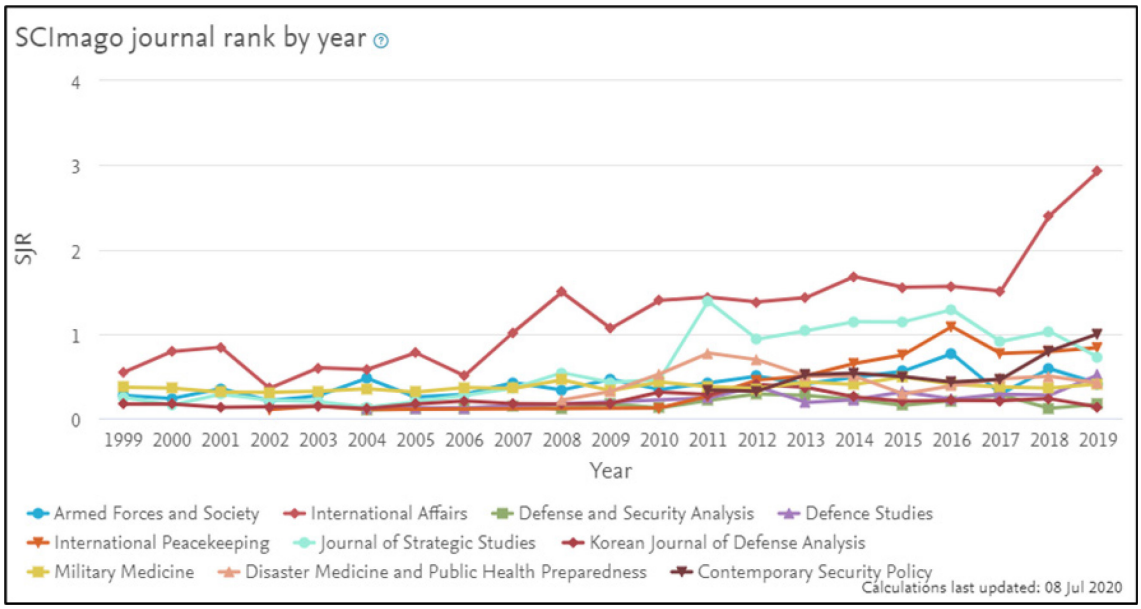

Figure 2-15: SCImago Journal Rank per Year of the Top Ten Journals in Phase Four (Scopus).

At first look at Figure 2-16, it appears that the top thirty authors have three or more publications post 2005 with the top author having 19 retained publications indexed in Scopus. Four of the authors in Figure 2-16 are also present in Figure 2-7 indicating that they likely not only have relevant publications on the research topic but likely also have expertise in related topics. Researchers wanting to identify experts for symposiums or consulting purposes may therefore want to further target these individuals more specifically, especially if the search has to be broadened with respect to the results arising from the final paper set.

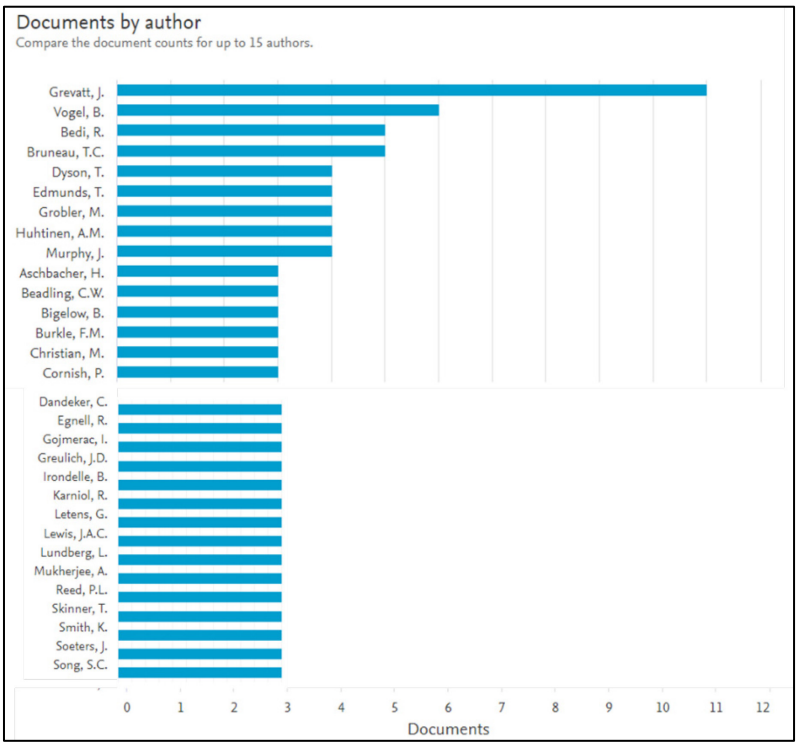

Figure 2-16: Authors with Three or More Publications in Phase Four (Scopus).

When considering Figure 2-17, one can establish that it is quite similar to the results in Figure 2-8 with the biggest change being the absence of China from the list.

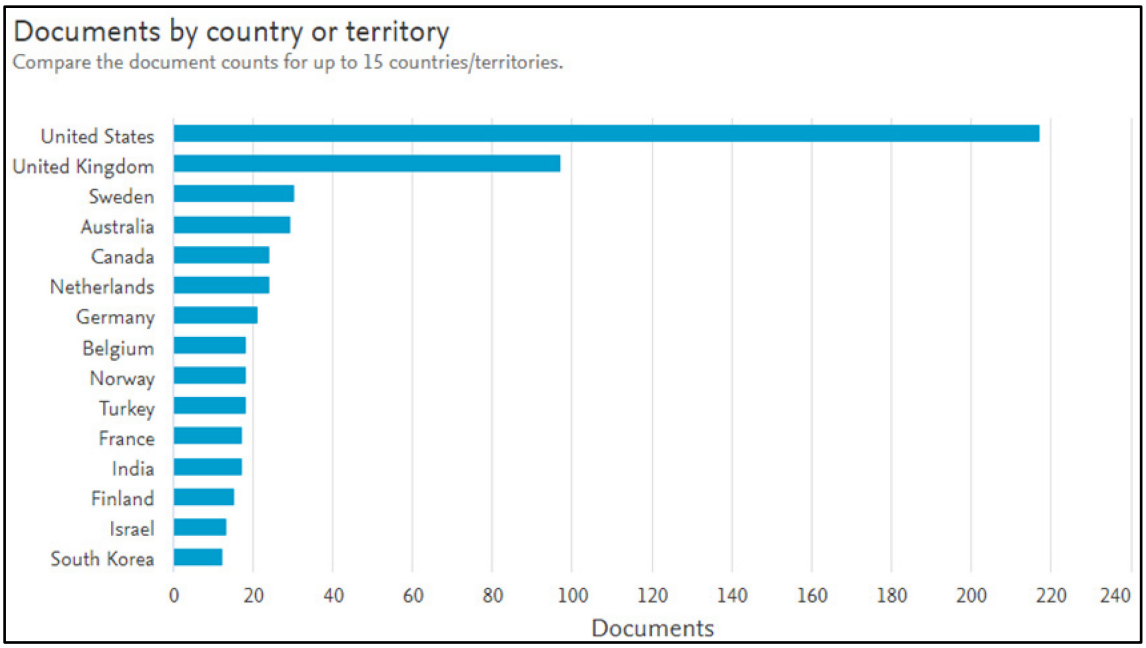

Figure 2-17: Number of Phase Four Documents per Top Fifteen Countries (Scopus).

Figure 2-18, also seems to indicate that not all more mature countries may are represented in the work group which again needs to be confirmed from the analysis of the final paper set.

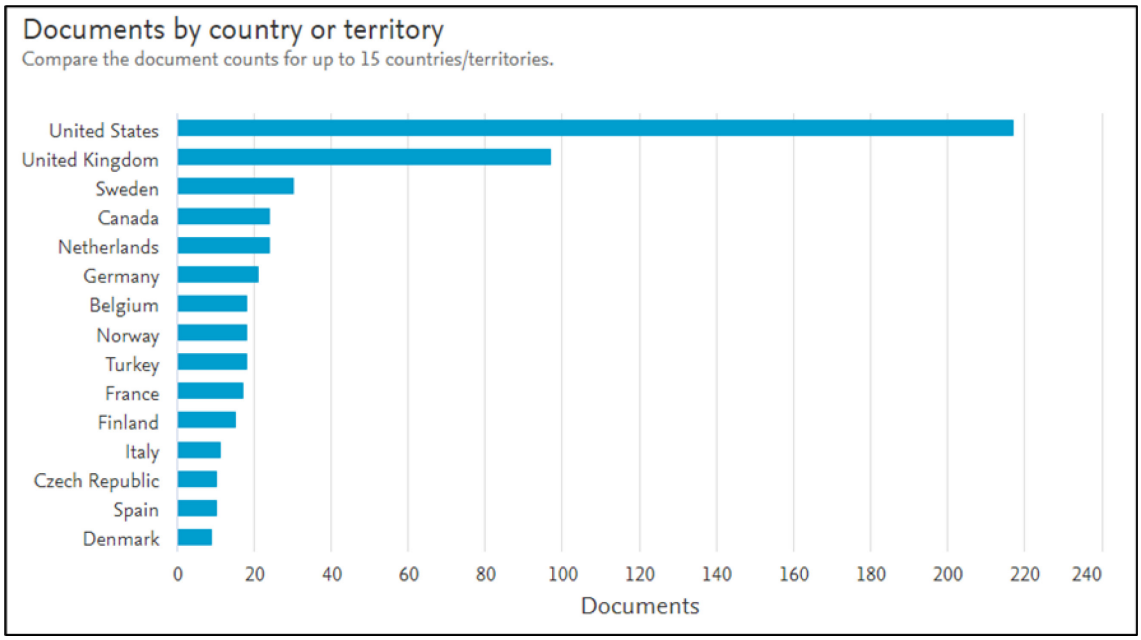

Figure 2-18: Number of Phase Four Documents per Top Fifteen NATO and EU Countries* (Scopus, 2005-2020, *Including Switzerland).

Finally, Figure 2-19 again emphasises the diversity of the research topic as characterised by the different Scopus subject areas the previously mentioned limitations notwithstanding.

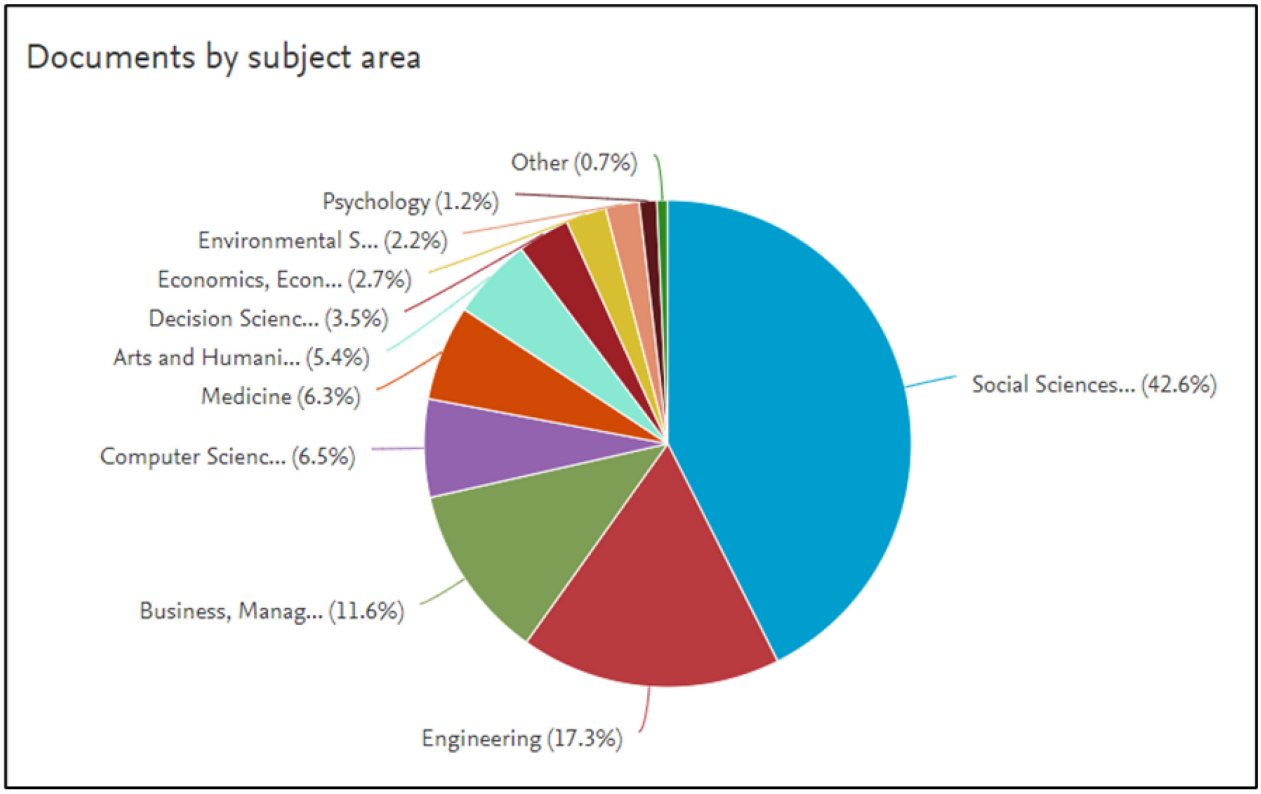

Figure 2-19: Catalogued Research Domains of Documents in Phase Four (Scopus).

In the second and final review process of phase five, the selected 739 documents were analysed based on a review of the full paper content including title, keywords, abstract, introduction, titles, sub-titles, figures, tables, conclusion, and annexes. In this way, one can determine if a document meets the established criteria [23]. Contrary to the previous phase, exclusion criteria were now strictly applied even if some researcher discretion was allowed regarding some magazine and book chapters that had been wrongly catalogued in the platforms as Journal papers. In addition, documents that did not adequately focus on defence organisations and comprehensive defence were excluded. The process was conducted by two researchers in parallel with divergence being resolved through consensus and discussion. Ultimately, a total of 147 papers were retained to which seven documents directly obtained from NATO SME's was also injected thereby constituting the final paper set (see Appendix 2-1). The bibliometrics of this final paper set presented in the next "findings" section was done using several tools. Besides using the tools available in Scopus which can only be applied to the results within this platform, MS Excel, and VOS Viewer, which is one of the leading bibliometrics programs currently available [38], were used. This implied the generation of a single RIS bibliometric file for the full data set using Mendeley library software.

Given the huge number of results in phase five originating from the wide range of disciplines, in phase six, it was not possible to perform synthesis on the full final paper set within the scope of this study. Therefore, a sub-set of papers was constituted for synthesis and analysis in order to address the research questions (other than bibliometric) and provide insights on the research topic. The criteria for paper prioritisation in the sub-set included the year of publication (to prioritise recent publications), prioritising publications touching on CA within NATO and EU countries, ensuring diversity in the research domain (such as cyber, diplomacy and crisis management), the prioritisation of journal publications over conference papers touching

on the same domains, ensuring a mix of academic and practitioner documents, and prioritising publications with a national instead of a purely supranational focus (as this better corresponds to the overall level of analysis of the NATO study which is the national comprehensive defence system). Further, data extraction was based on the research questions and performed in two ways simultaneously: via MS Excel and MS Word with similar information being extracted from documents through both means. Collection via MS Word was more extensive compared to MS Excel which was more keyword based. The various columns for the Excel document and the various subheadings for the Word document were divided into two parts: a general part and a part specific to each stakeholder identified.

2.4 FINDINGS

2.4.1 Characteristics of the Research Area: Bibliometrics on the Final Paper Set

The following tables and figures depict the results of phase five from the Scopus platform, VOS Viewer and MS Excel. Whereas the Scopus graphics are only valid for the Scopus sub-set of papers and this is then clearly indicated in the exhibit caption, the VOS Viewer and MS Excel results are valid for the full final paper set including documents submitted by the SME's. Table 2-2 presents the distribution of the different document based on the document type and the platform of retrieval.

Table 2-2: Final Paper Set per Platform or Source (N).

	Scopus	NATO Library	SharePoint	Subject Matter Experts	Total
Article	106	5		2	113
Conference paper	16			1	17
Report	1			3	4
Thesis			5		5
Book chapter	1		1	1	3
Magazine	3	1			4
Research paper	0		4		4
Working paper	1				1
Other	1	1	1		3

From Figure 2-20, and in comparison with Figure 2-12 and Figure 2-3, the percentage of conference papers retained has not varied significantly between the final paper set and the initial review for the Scopus-subset (not presented to avoid redundancy). This indicates that the likely quality differences between journal articles and some conference papers was resolved during the initial review phase. These numbers are slightly lower for the full final paper set due to the inclusion of other type of documents originating from SMEs and SharePoint.

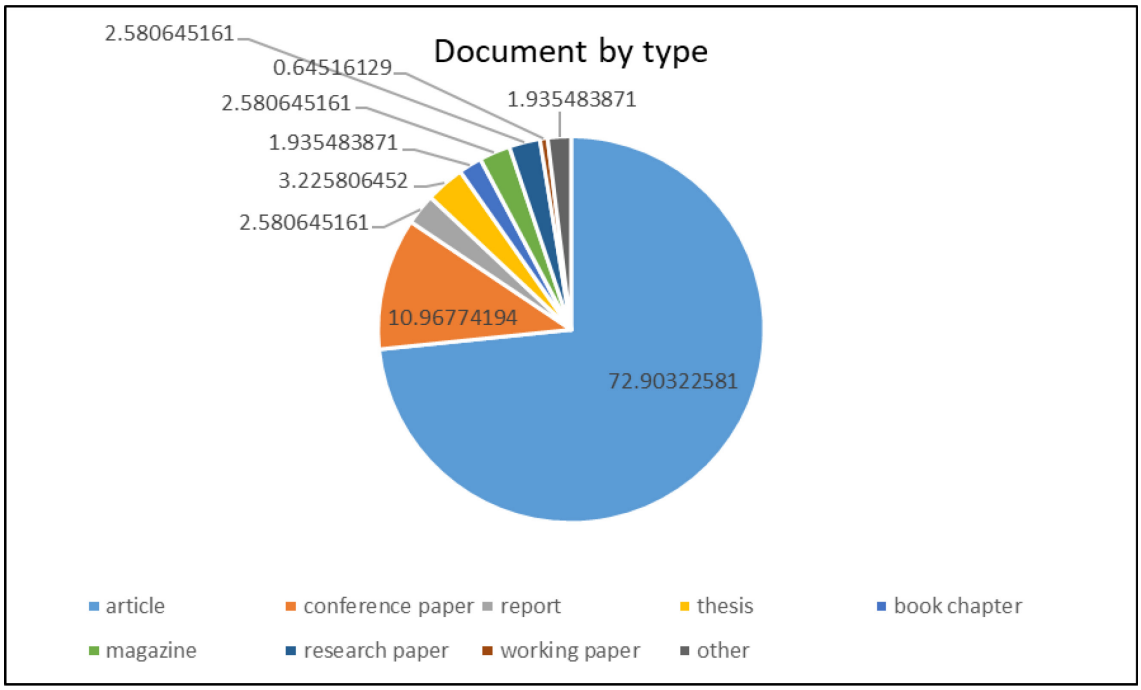

Figure 2-20: Types of Final Paper Set Documents.

Next, from Figure 2-21, and in comparison with Figure 2-11, it appears that we have found recent publications relevant at a higher rate as compared to the results of Phase four. The spread of the papers over the years in the final paper set is however similar to the trend of the initial search results of Figure 2-2. The trend is heavily influenced by and is similar to the one arising from the Scopus sub-set which is also not presented to avoid redundancy. Note that in the figure data from the year 2020 has been voluntarily suppressed.

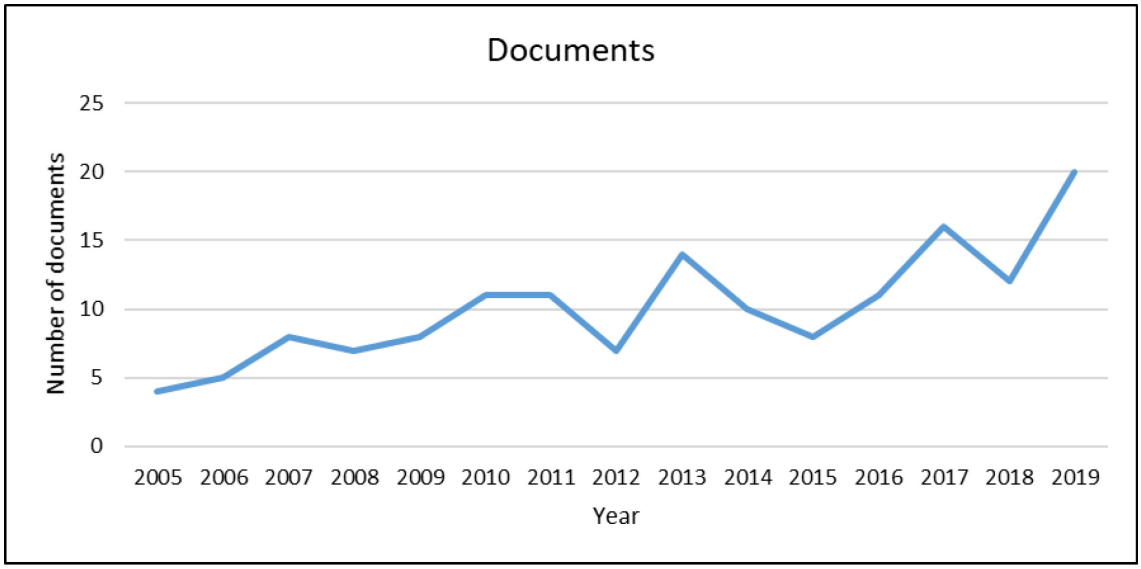

Figure 2-21: Number of Documents per Year in the Final Paper Set.

The next three figures are specific to the Scopus sub-set.

When comparing Figure 2-22, Figure 2-13 and Figure 2-4, we find that the documents retained originate from some of the same journals previously reported even if there are again changes in the ranking. International Affairs, Korean Journal of Defence Analysis, Military Medicine, Contemporary Security Policy are now replaced in the top ten which consists of the following: Defence Studies, Defence and Security Analysis, Disaster Medicine and Public Health Preparedness, Small Wars and Insurgencies, International Journal of Emergency Management, Armed Forces and Society, Journal of International Peacekeeping, International Peacekeeping, Journal of Humanitarian Logistics and Supply Chain Management and Journal of Strategic Studies. In doing so, the final paper set seems to originate more closely from journals focused on defence matters, emergency management and strategy.

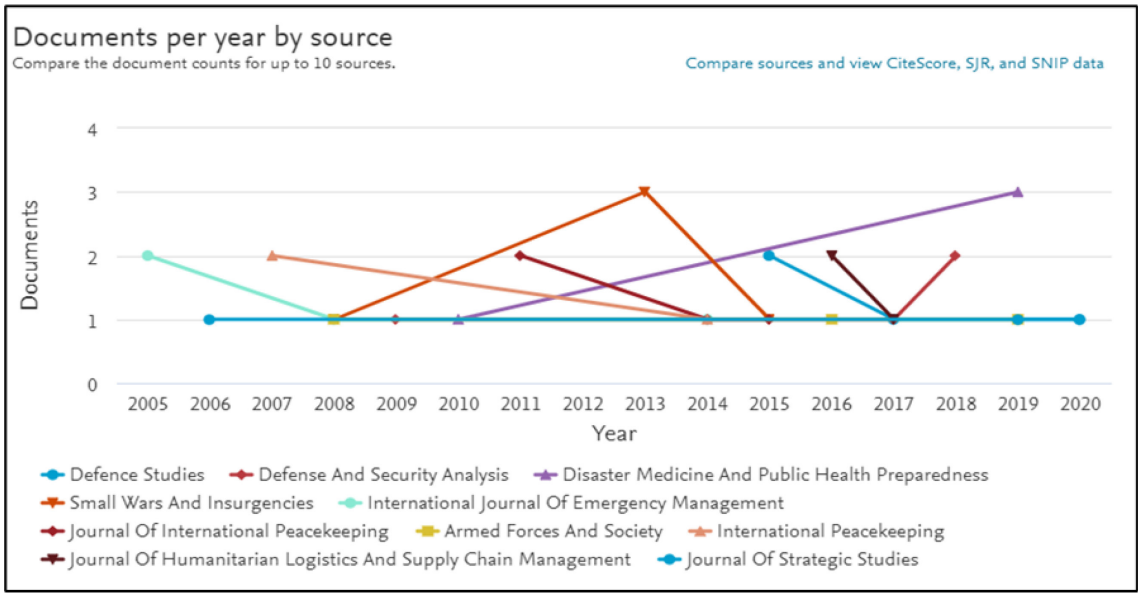

Figure 2-22: Number of Final Paper Set Documents Published per Year in the Top Ten Journals (Scopus).

Contrary to Figure 2-4, Figure 2-5, Figure 2-6, Figure 2-13, Figure 2-14 and Figure 2-15; Figure 2-22, Figure 2-23 and Figure 2-24 do not appear to show a clear favourite in terms of the number of articles published on the topic. Researchers may therefore want to consider the individual impact factor of the journals depicted in Figure 2-23 and Figure 2-24 when considering a submission process. Most journals have a CiteScore for 2019 between one and two with the Journal of Humanitarian Logistics and Supply Chain Management having the highest score (4.1) followed by the Journal of Strategic Studies (3) and International Peacekeeping (2.6). The SCImago rankings in Figure 2-24 show similar results for 2019 with the highest impact factor journals being the Journal of Humanitarian Logistics and Supply Chain Management (0.894) followed by International Peacekeeping (0.839), Small Wars and Insurgencies (0.736) and the Journal of Strategic Studies (0.723). Both Figure 2-23 and Figure 2-24 show the impact factor of the top ten journals to be increasing across the years which is positive for the field.

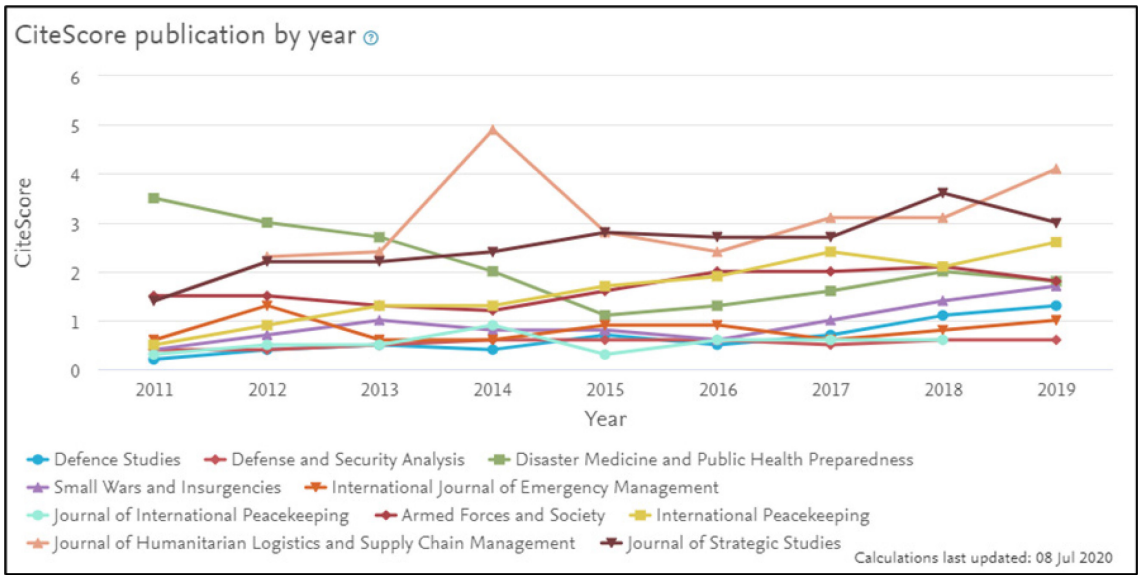

Figure 2-23: CiteScore per Year of the Top Ten Journals within the Final Paper Set (Scopus).

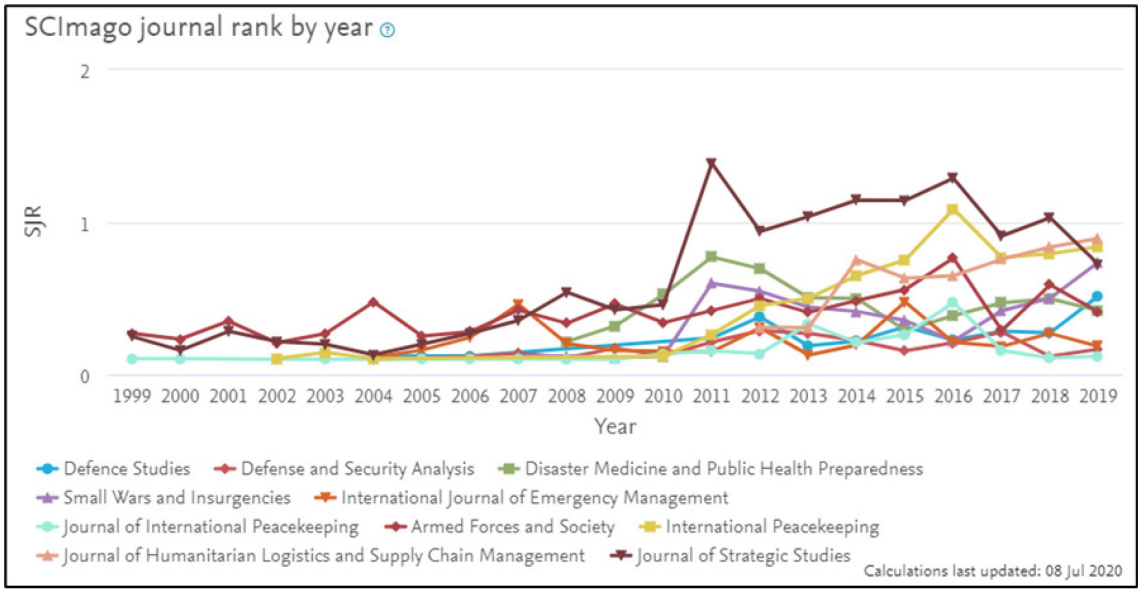

Figure 2-24: SCImago Journal Rank per Year of the Top Ten Journals in the Final Paper Set (Scopus).

As far as authors are concerned, on first look at Figure 2-25, it appears that 25 authors have two or more publications in the final paper set with only three authors having three publications. This implies that most authors have a single publication on the research topic after which they move on to another (likely related) topic. Interestingly, twelve authors (Beaton, Boiney, Drury, Egly, Gordon, Henriques, Kanenberg, Klein, Matei, Morton Hammer, Rietjens and Wallenius) are cited in Figure 2-25 but not in Figure 2-16 indicating that they may be focussing more closely on the research topic only. So, one may also want to investigate the publications and exact subject areas of these twelve authors specifically when trying to identify experts for consultancy purposes. Figure 2-26 depicts the co-authorship network within the final paper set which indicates the existence of three clusters depicted by the different colours. The strength of a link between any two authors or items is depicted by thickness of the line between them in such a way that the strength of any

line represents the number of documents any authors have published together. While the clusters seem to be connected by at least one author, it may be interesting to weigh representation from each cluster for consultancy purposes. Similarly, Figure 2-27 weighs the results of Figure 2-26 by average publication year meaning that it depicts a more active cluster with respect to another cluster [51]. For example, if two authors have co-published one document each in 2020 and 2018, then the average publication year of the link between them is 2019 and the link is coloured appropriately.

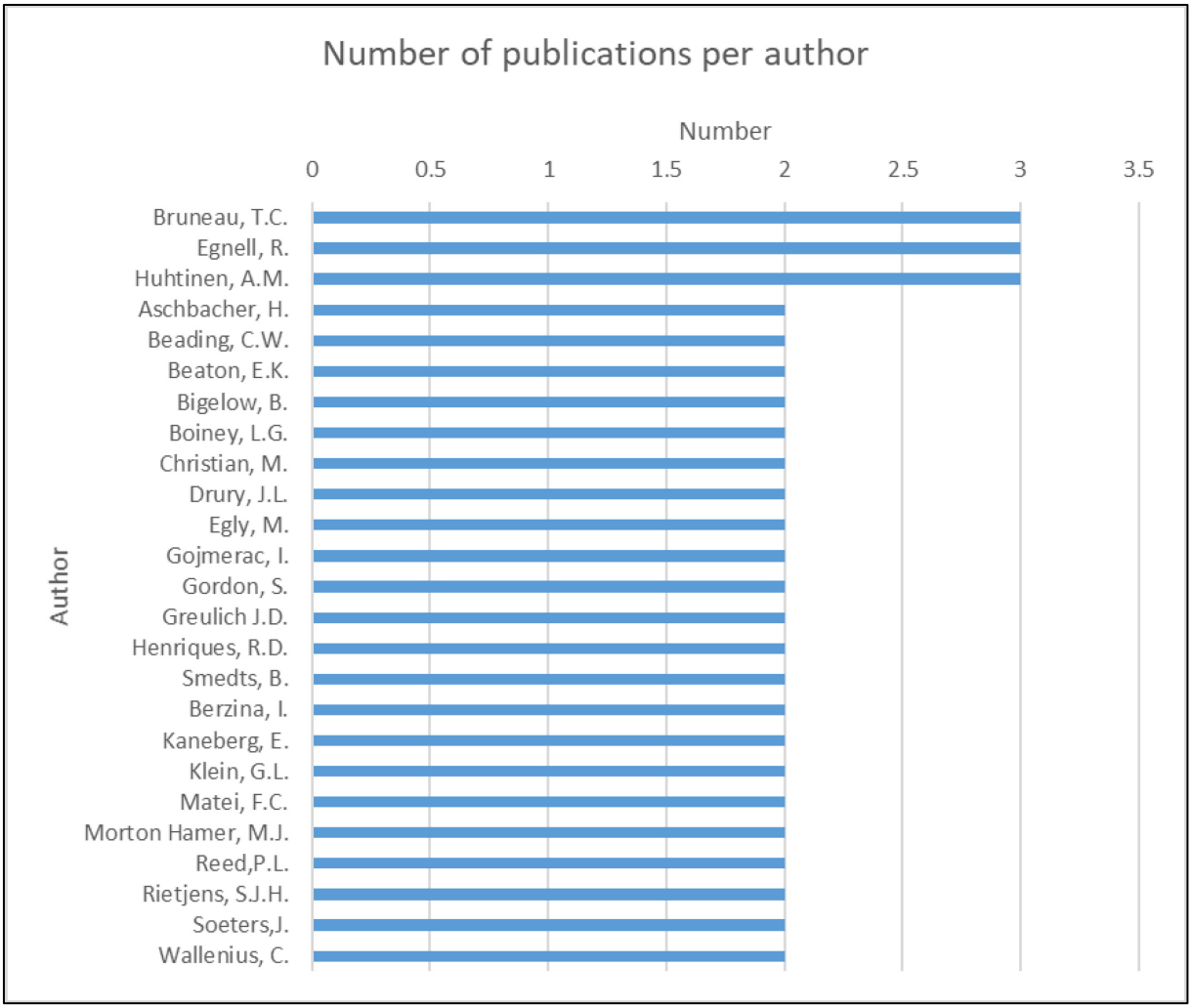

Figure 2-25: Number of Authors with Two or More Publications in the Final Paper Set.

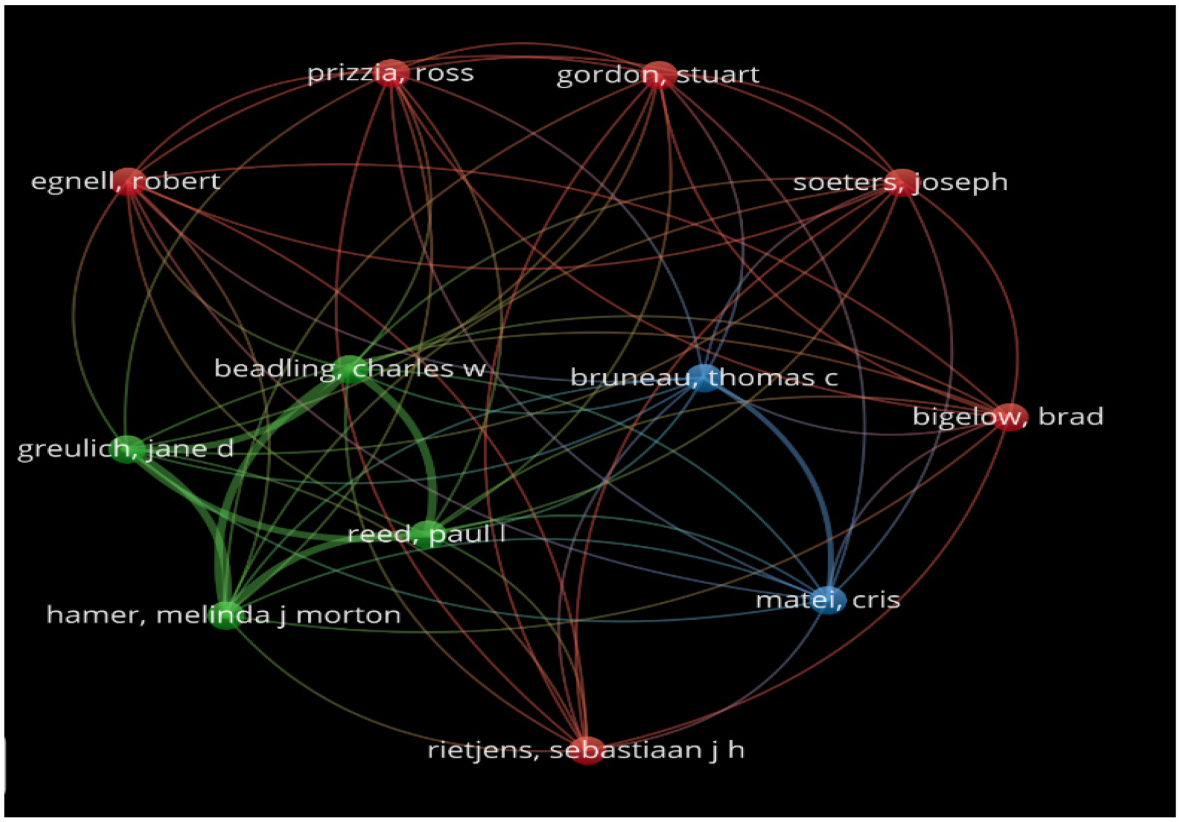

Figure 2-26: Co-Authorship Network Within the Final Paper Set.

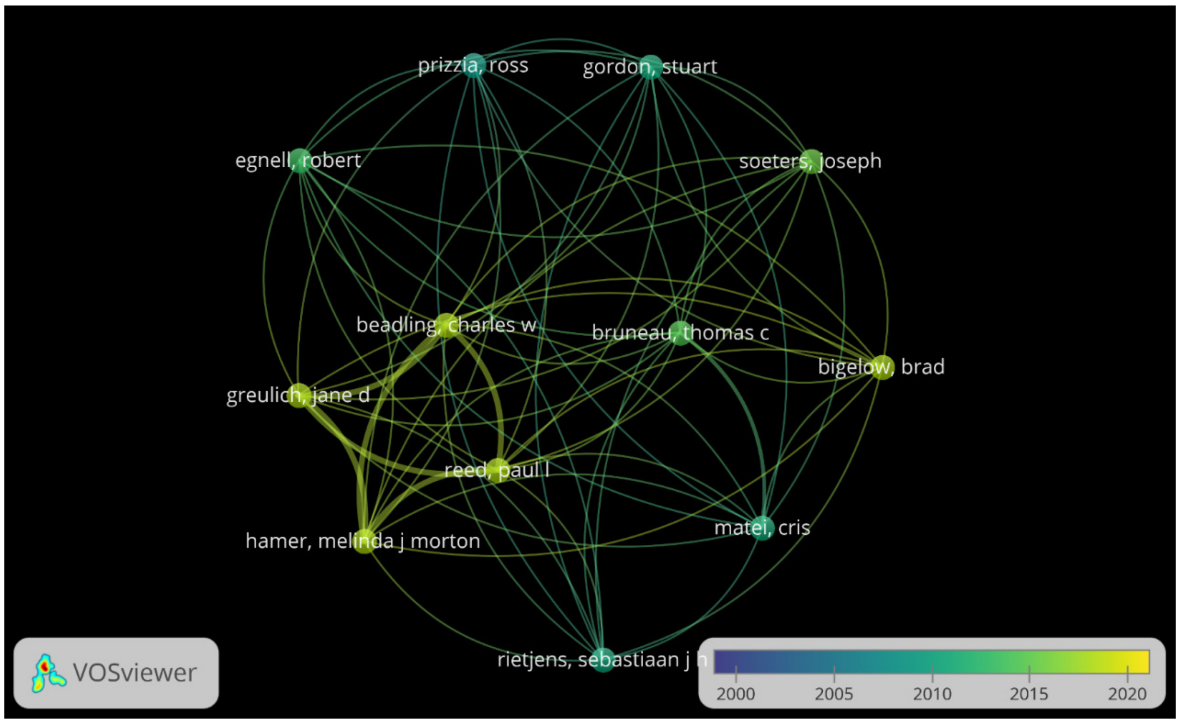

Figure 2-27: Co-Authorship Network Within the Final Paper Set Weighted per Average Publication Year.

Figure 2-28 represents the number of final papers (set documents) for the top fifteen entities (either countries, regions, or organisations) as qualitatively assessed by the researchers based on the document content. The main difference with Figure 2-29, which is the same graphic for the Scopus results, pertains to the method of counting in Scopus which is not clear and may be based on authors' origin. Compared to previous figures such as Figure 2-17 and Figure 2-18, Figure 2-28 indicates that our final paper set is more diverse from a contextual viewpoint than previous results indicate with generic results, supra-national results and warzones all finding inclusion in the top fifteen list. As such, NA in Figure 2-28 denotes that a document is based on generic concepts and does not specifically limit itself to any entity or country. In addition, 'EU' denotes instances where the document specifically limits itself or pertains to issues related to the European Union such as the Common Security and Defence Policy. The same is the case for NATO. One dysfunctionality of Figure 2-28 and the underlying results however is the higher representation for Belgium that is due to the inclusion of papers from SharePoint which is a purely national database with very few exceptions. We also have to keep in mind that a disproportional number of researchers publishing on NATO and the EU may also be of Belgian origin due to the geographical proximity of the country and these two institutions.

Figure 2-30, which depicts the top fifteen NATO and EU Countries depicted in the final paper set nuances previous indications about participation of mature countries within the work group while indicating that the USA and the Netherlands are probably the countries being missed the most due to which they may be specific targets for inclusion in future initiatives. These results are similar for the Scopus sub-set which are not presented to avoid redundancy.

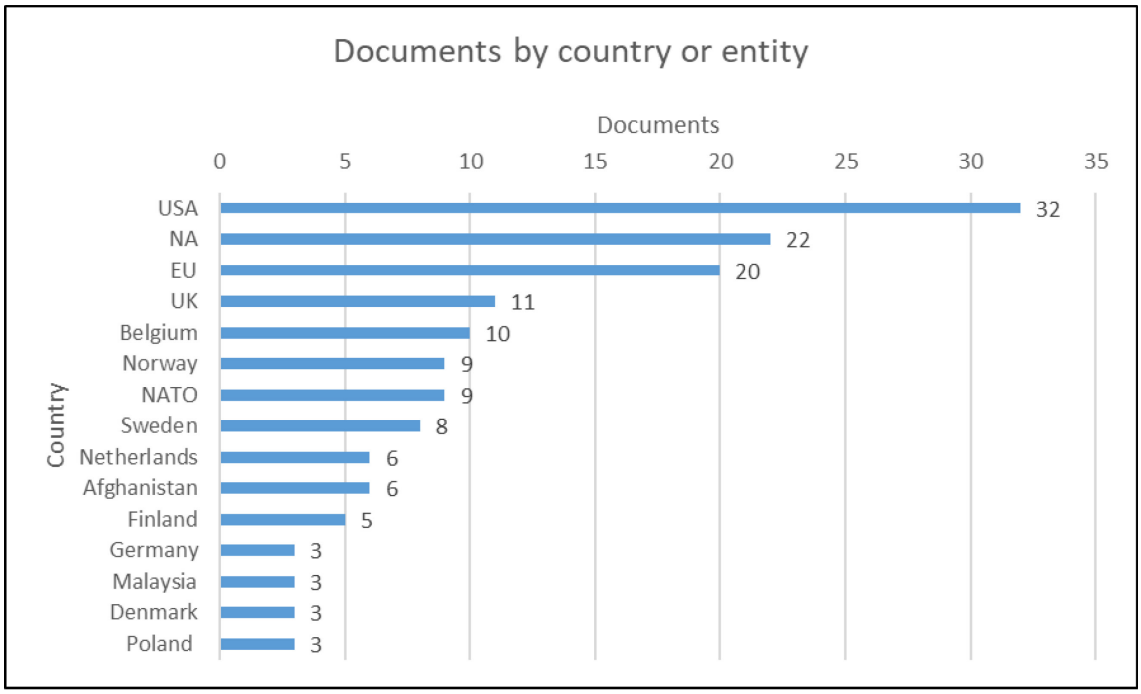

Figure 2-28: Number of Final Paper Set Documents per Top Fifteen Countries or Entities.

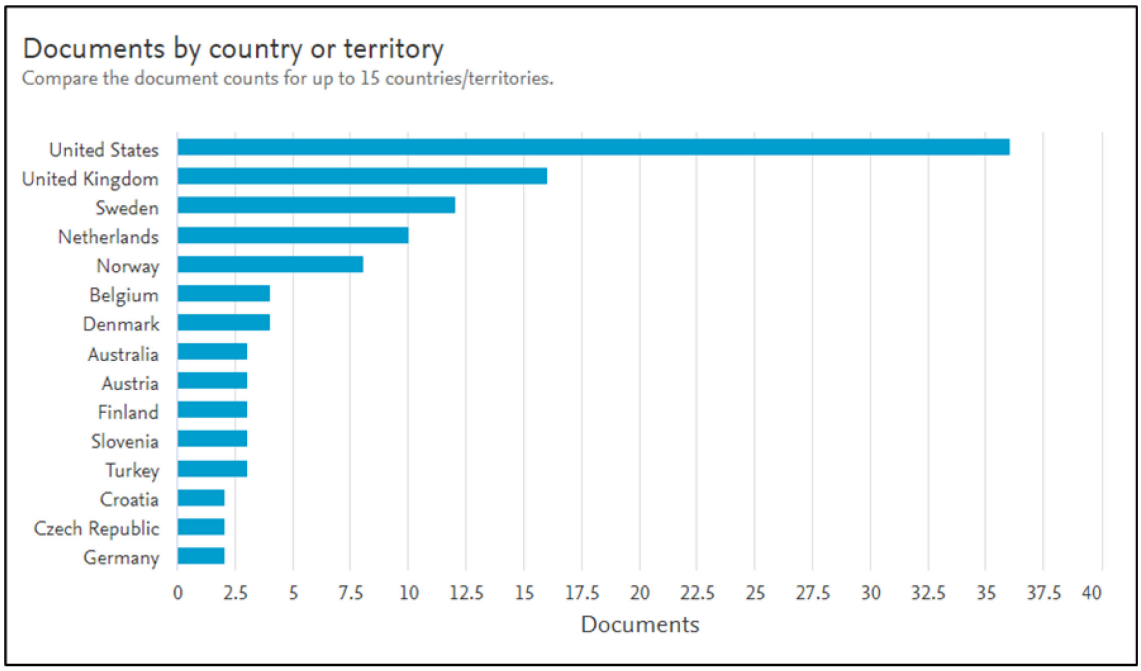

Figure 2-29: Number of Final Paper Set Documents per Top Fifteen Countries (Scopus).

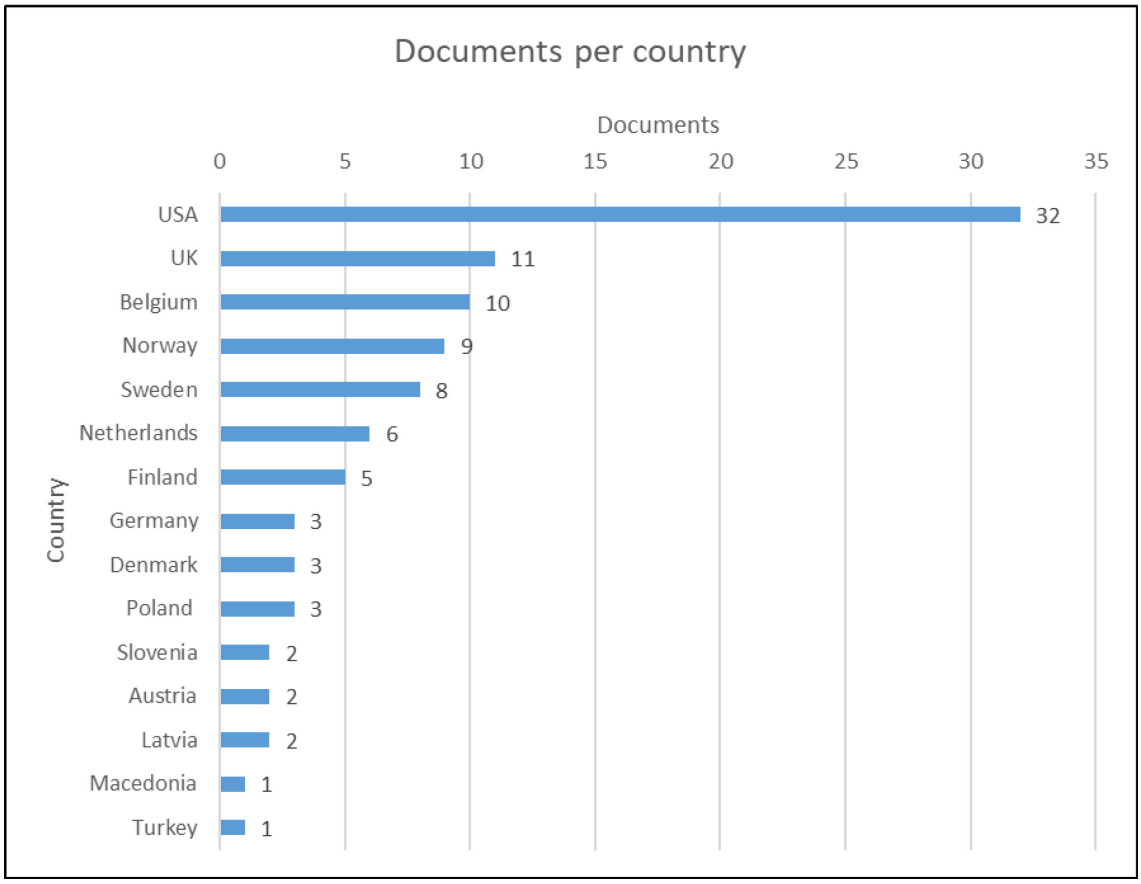

Figure 2-30: Number of Final Paper Set Documents per Top Fifteen Countries or Entities Within NATO and the EU.

The next figure, Figure 2-31 is limited to Scopus results and is subject to Scopus limitations in such a way that (even if the overall portrayal seems coherent with our final data set) the categorisation of a plurality of documents under "social science" is too vague to draw any definite conclusions. Some of the functionalities of VOS Viewer applicable to the full data set offer an alternative means to better understand the categorisation and the content of the final dataset, however. First, Figure 2-32 portrays a co-occurrence map of the keywords contained within the bibliographic data of the final paper set. For the purpose of this exercise, we set the minimum number of co-occurring words to three, which generated 44 terms meeting the threshold. After verification for trivial spoilers such as "a" and "the", this resulted in 39 relevant items retained being disaster preparedness, coordination, security, civil, civil-military, Ebola response, humanitarian aid, CSDP, disaster management, community, European Union, military cooperation, operations, planning, EU, international security, situation awareness, Africa, civil-military cooperation, collaboration, disaster response, foreign policy, interoperability, peace operations, peacebuilding, resilience, cybersecurity, homeland security, management, coercion, crisis management, military, military relations, terrorism, Afghanistan, cyber security, and civil-military relations. Some of the keywords are obviously redundant and applying subjective judgement to cluster the results indicates that the following domains may constitute the key research domains for this topic: Disaster and crisis management, interagency cooperation (to include interoperability and planning issues: national, international, civil, military, civil-military…), civil-military relations, terrorism, cybersecurity, conduct of operations, delivery of humanitarian and developmental aid, foreign policy and international security, EU crisis response mechanisms, and national or homeland security including situational awareness and resilience. Note that the results are largely similar using a variety of options in VOS Viewer including the method (fractional or full) and the attribution of score (links, total link strength and occurrences) [51].

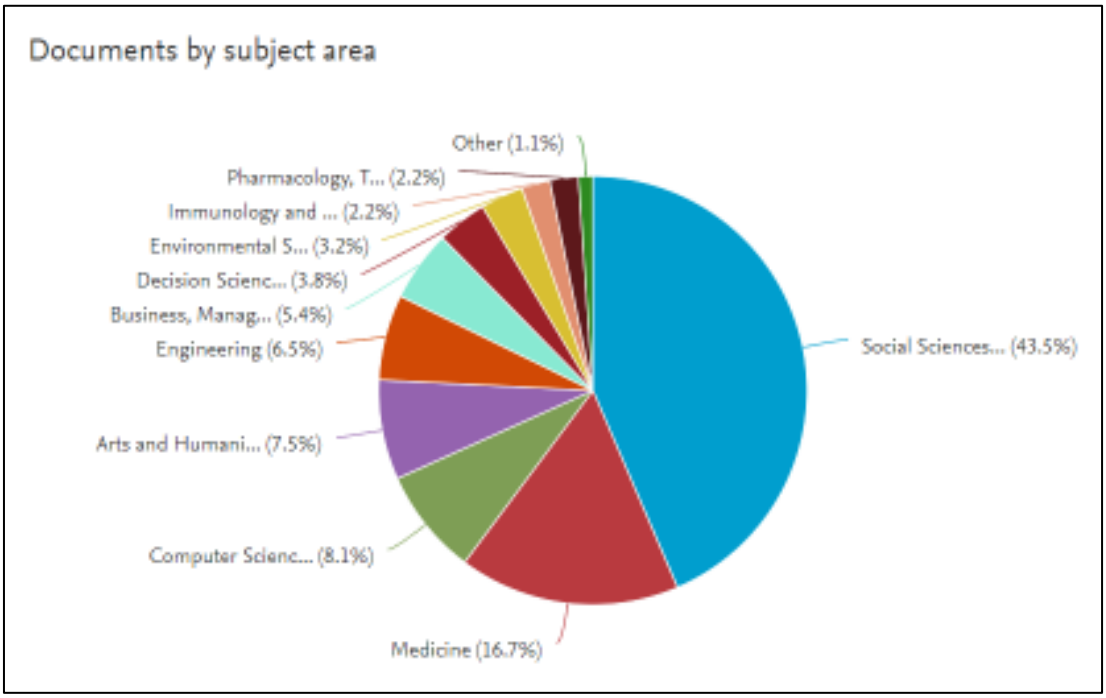

Figure 2-31: Catalogued Research Domains of the Final Paper Set Documents (Scopus).

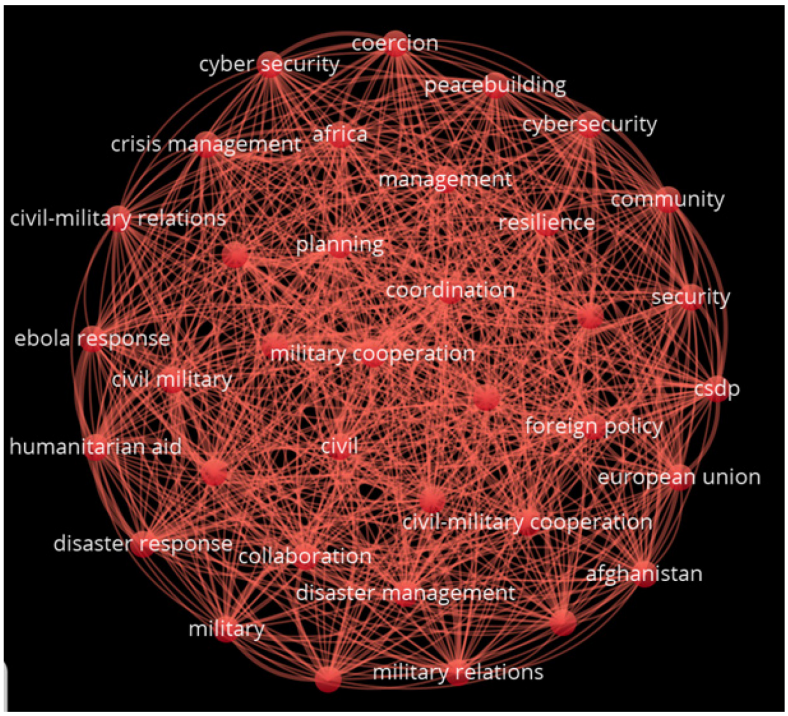

Figure 2-32: Co-Occurrence Map of Keywords in the Final Paper Set (Bibliographic Data).

Figure 2-33 is the same map that is now weighted per average publications per year indicating that items such as terrorism and cybersecurity may be amongst the "hotter" items.

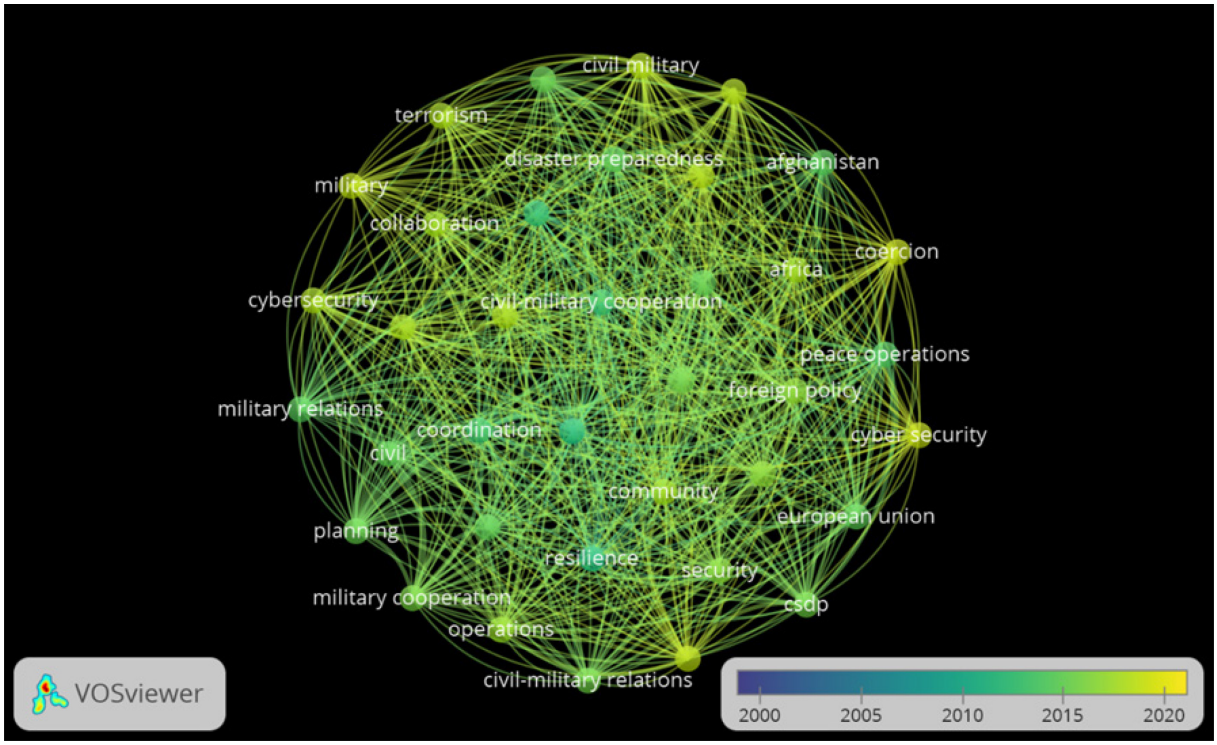

Figure 2-33: Co-Occurrence Map of Keywords in the Final Paper Set Weighted per Average Year of Publication (Bibliographic Data).

Figure 2-34 and Figure 2-35 further depict how some of these key domains may be connected. First, Figure 2-34 is a co-occurrence map based on text data of words occurring in the title within the final paper set. For generating this map, we selected a binary method of calculation with a minimum occurrence of two words. This resulted in 56 retained items with only the linked items being shown. The weight is attributed based on occurrence but other options such as weightage based on links and total link strength yield similar results. Next, Figure 2-35 is a similar co-occurrence map based on full counting instead of the binary method that yields more items and links. Again, the minimum occurrence was set to two and the weightage was based on occurrence. Other options such as weightage based on links and total link strength yield similar results here as well. This yielded 115 items that were then verified for the usual disruptors. Again, only the linked items are depicted in the Figure. As such, Figure 2-31 to Figure 2-35, confirm the presumed diversity of the research topic as depicted in the previous results.

Overall when assessing the overall maturity of the research area, and given; the fact that the research field is not yet clearly defined, the fact that publications arise from a diverse set of domains ranging from medicine to international policy, the fact that the topic does not have its own clearly identified Journals, the fact that most authors only have single publications, the fact that only a small amount of co-authors exist with not many joint publications leads us to consider these as indicators pointing to a research area with a low maturity level [24]. When combined with the increasing number of publications over time, and the increasing impact factor of the most prominent journals, this points to a still developing research area.

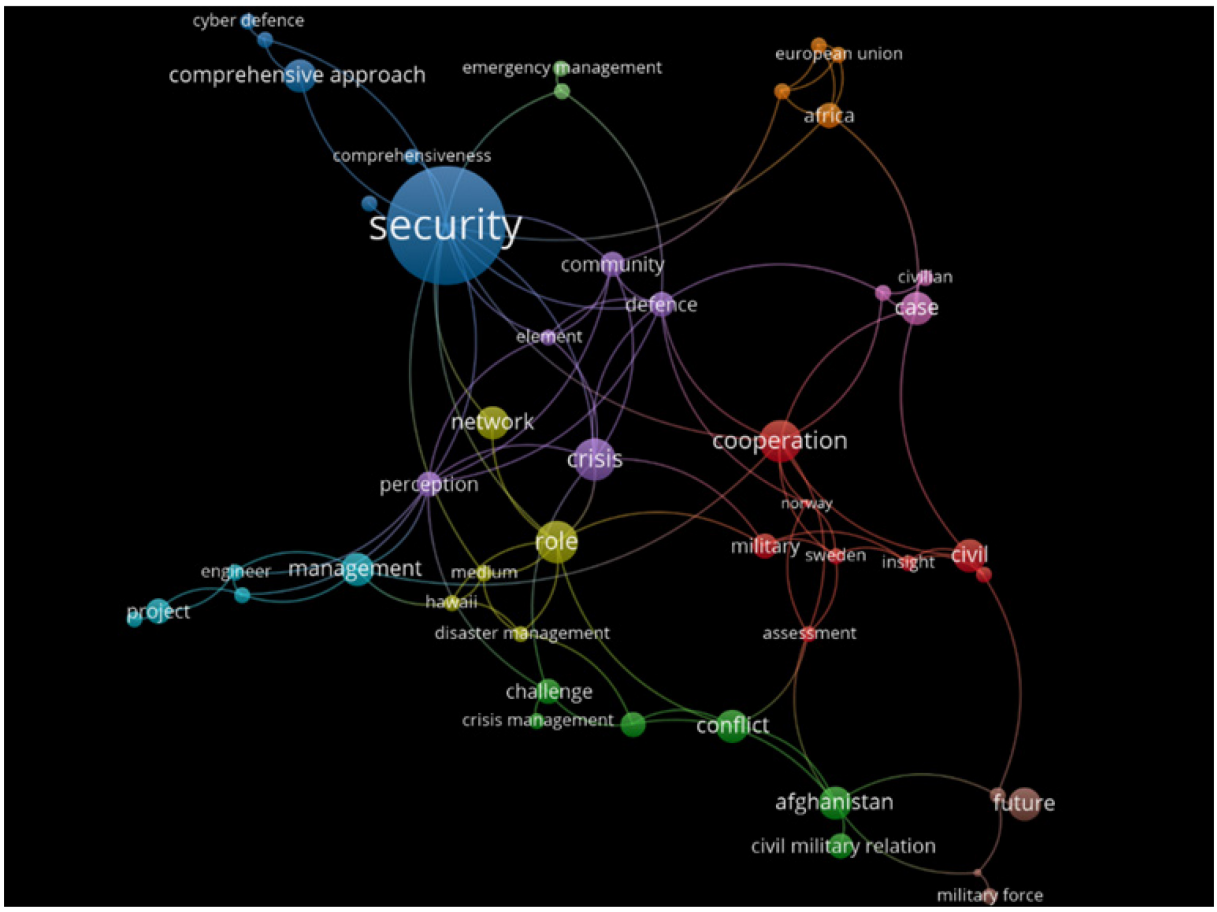

Figure 2-34: Co-Occurrence Map of Words Within the Final Paper Set (Title, Binary Counting).

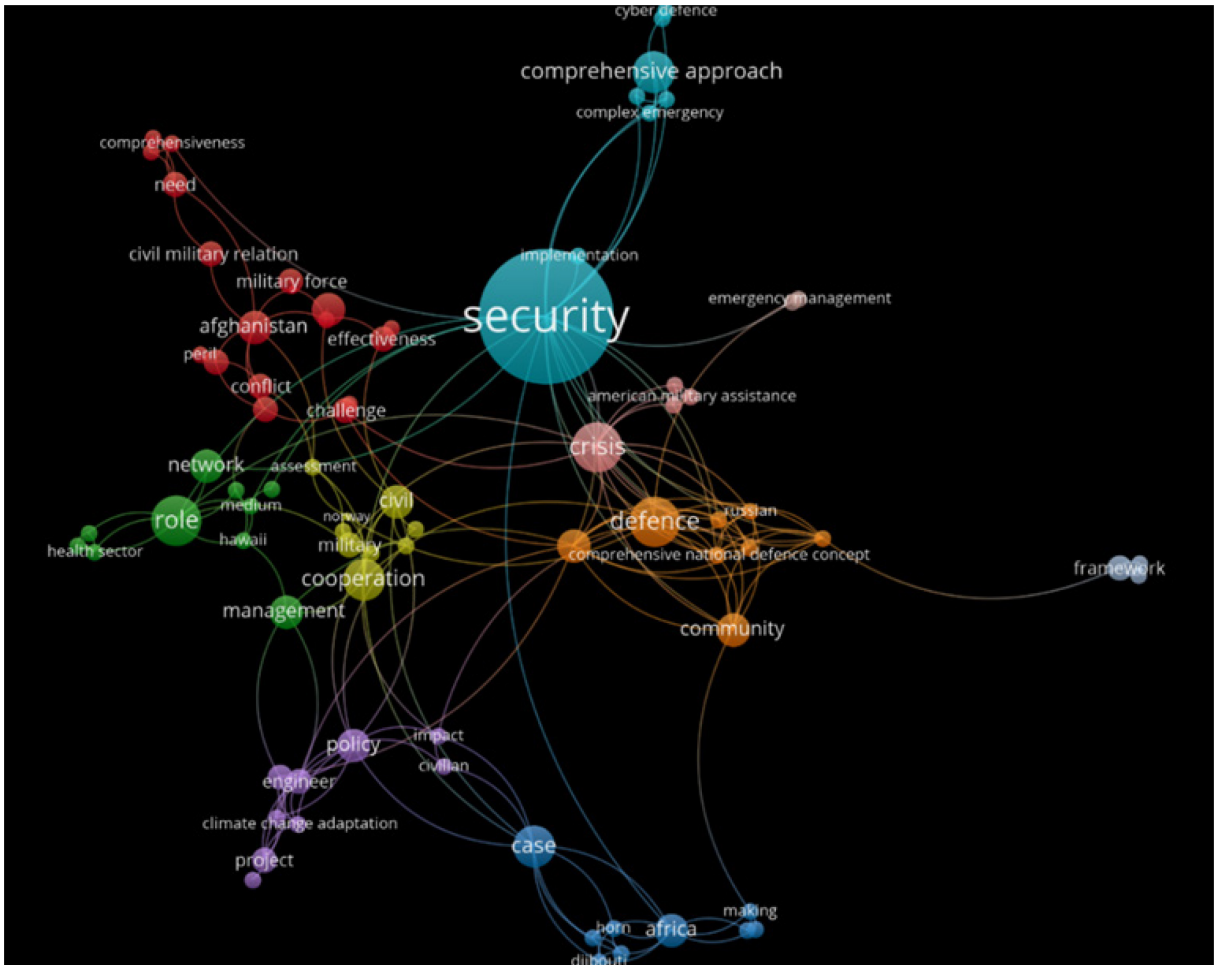

Figure 2-35: Co-Occurrence Map of Words Within the Final Paper Set (Title, Full Counting).

2.4.2 Actors and Stakeholders: Identification, Classification and Description

The effectiveness of an organisation depends on the ability to choose objectives that are worthwhile for both the organisation and the strategic stakeholders [44]. In order to be able to select these objectives, it is important that the organisation have a good knowledge of the relationships with the most important stakeholders which is why we study them in more detail in this section. Identifying stakeholders and linking them with some of the previously mentioned CA concepts should enlighten us as to the approaches used and their comprehensiveness within various countries.

2.4.2.1 Stakeholder Identification

Before starting to identify stakeholders active within a comprehensive national defence system, we first had to precisely define the concept of stakeholder itself. The most commonly used definition of a stakeholder is the one originating from Freeman: *"any group or individual who can affect or is affected by the achievement of the organisation's objectives"* [9], [18], [22], [36]. In a military and security context, a stakeholder is therefore someone or an entity that has an influence on defence and security organisations, but also who can also be influenced by them. We further narrow the understanding of this definition to correspond to the focus of our study. In doing so we exclude "negative influencers" such as countries posing threats who can obviously also affect and be affected by the defence and security organisations. Stakeholder identified based on this definition were then categorised based on information found in the underlying documents or based on researcher

judgement. For each stakeholder or stakeholder type, we also tried to identify the important roles, responsibilities, and expectations they may have with respect to defence and security organisations.

2.4.2.2 Ministries and Departments

The first stakeholder identified was Ministries or Departments (based on the country) with the most common Ministries identified being the ones interacting within a 3D framework: Defence, Foreign Affairs, and International Aid [27]. Amongst others, the 3D approach was found to apply in the United States, the United Kingdom, and the Netherlands with the main stakeholders besides Defence being:

- United States of America (USA): Department of State and United States Agency for International Development;
- United Kingdom (UK): Foreign and Commonwealth Office and Department for International Development; and
- Netherlands: The Ministry of Foreign Affairs and the Department for Development Cooperation.

2.4.2.3 Political Level Stakeholders

Still on the national political scene, various concepts on civil-military theory were found in the literature. Terms such as Civil-Military Coordination (CMCO), Civil-Military Relations (CMR) or Civil-Military Cooperation (CIMIC) seem to be used interchangeably. Whereas CMR and CMCO tend to deal with the relations between politicians, the military and society at the national and strategic levels, CIMIC seems to focus on operations at the tactical level [16], [39].

A recurring issue in the theory of civil-military relations especially important for non-established democracies is the one relating to civilian control of politicians and civilians over the armed forces and the security apparatus with the theories of Huntington and Janowitz enjoying prominence [15], [16]. According to Huntington, there should be a clear separation between policymakers and the military that is necessary to maximize military professionalism and effectiveness [15]. Contrary to this current, the doctrine of Janowitz assumes greater integration and interaction between political and military leadership in order to achieve adequate coordination and mutual trust [16]. According to Kiszely, military organisations tend to be in favour of objective control as prescribed by Huntington whereas Governments tend to be more in favour of a so-called subjective control as prescribed by Janowitz [25].

While in some documents the relationship between politicians and military organisations is described in a rather general way, in other documents, specific stakeholders can be found. For example, Wallenius et al., mention the Swedish political elite in a rather general sense even if it can be determined that this includes the Government, Ministers, Party leaders, Members of Parliament and Parliamentary Commissions and Cabinet-level staff [53]. As such, the Government and the Ministers of the various departments previously identified can be emphasized [15], [16]. Still in some countries such as Belgium, Party leaders may be even more important.

These political stakeholders have many roles and responsibilities in the security domain, and although a complete analysis is outside the scope of this study, several important responsibilities were identified within the final paper set. First, the responsibility for ensuring and implementing a balanced defence policy can be cited [15], [16], [52]. Second, politicians have the responsibility to inform society about the importance and mission of the security forces [53]. Third, it is important for security organisations to have political support during changes and transitions in the security architecture. On the one hand, defence and security organisations may be critical of defence policy drafted by politicians who show little interest in national defence and have a rather limited knowledge of defence in general [53]. On the other hand, one must admit that it is difficult to draw up a clear defence planning if the threats are themselves rather vague and unpredictable.

2.4.2.4 National Coordinating Bodies

The various national coordinating bodies, such as those coordinating crisis response measures between the different departments, could perhaps have been mentioned in the previous category but we have chosen to mention them separately keeping stakeholder characteristics such as saliency, power, and urgency in mind. Examples of such coordinating bodies found included:

- The Cabinet Office of the United Kingdom; and
- National Security Councils of the United Kingdom and the United States of America.

In the British system, the Cabinet is responsible for coordination between the various government departments and is therefore not limited to the Prime Minister. It can be seen as a coordinating body but bears ultimate responsibility and has real decision-making power affecting the whole of Government [15]. The British National Security Council on the other hand has a more coordination type of function with its mission being to ensure that the security of the United Kingdom is dealt with in a global and strategic manner [50]. The National Security Council in the US is similar to its UK counterpart as it was created to integrate the various facets such as diplomacy, defence and economics so that a unified national security policy could exist, [3], [16]. In practice, it is an advisory body that mainly advises the president and thus has little decision-making power [16]. Usually, an organ such as the National Security Council consists of the National Security Advisor, the most important Ministers or Secretaries, and the head of Government who also leads the body [50]. According to Kiszely, the formation of such a body can be an important step in providing a coordinated response to threats and in formulating a National Security Strategy or NSS [25].

2.4.2.5 International Organisations

International organisations also play an important role in the cooperation that exists between defence and security organisations. The most prominent, impactful, and well know are the European Union (EU) and the North Atlantic Treaty Organisation (NATO) and will be further discussed. Other organisations mentioned in the final paper set include the United Nations Organisation (UNO) and the Organisation for Security and Collaboration in Europe (OSCE).

In elaborating its vision of collective defence and collective security, NATO mainly has a coordinating role. Because NATO, as a politico-military organisation, only has a limited number of instruments at its disposal, it is obliged to call on the capabilities of the member to achieve collective objectives [13], [49]. With the aim of building up the necessary resilience of its member states, NATO has currently drawn up seven base line requirements. In this way, NATO shows what the requirements are that a country has to meet to be resilient against future threats [52]. In turn, it is a national responsibility to implement adequate measures in the national plans and report on them through the NATO Defence Planning Process (NDPP). In doing so, the NDPP four-yearly questionnaire is an important tool allowing nations to report on the status of implementation of measures in relation to NATO's strategic objectives and thereby is critically important for NATO to evaluate where it stands an organisation with respect to capabilities and resources [52]. Besides this main mechanism between NATO and Member States, several other mechanisms arising within the NATO context are worth mentioning:

- Host Nation Support mechanisms or HNS to achieve deployment and sustainability objectives;
- Framework Nations Concept (FNC) in the field of large-scale equipment projects and capability generation;
- Joint Expeditionary Force (JEF) in the field of generation of ready for elements; and
- Security Force Assistance (SFA) in the field of defence and security cooperation.

Contrary to the collaborative structures mentioned in the next sub-section that are mainly built on consensus, often a dominant stakeholder can be identified such as Germany in the case of several FNC initiatives or

the UK in the case of the JEF. First, from a NATO perspective, the missions, and exercises within the framework of Host Nation Support offer an opportunity to strengthen deterrence and to increase interoperability [42]. Second, the Framework Nations Concept (FNC) is a German initiative that aims to gather a large group of countries into clusters to fill capacity gaps [46]. In the beginning, the aim was to create capabilities in areas such as logistics in which there were shortages but eventually the aim became to cover the full range of NATO requirements [46]. The driving idea behind FNC is that only a number of large European states will have a broad spectrum of military capabilities at their disposal. These large states can then act as leading nations to coordinate clusters of military capabilities where smaller states would be able to join. Third, the Joint Expeditionary Force (JEF) is a UK initiative aimed at deploying a rapidly deployable force capable of carrying out the full spectrum of operations. As the British want to keep their independence as much as possible, they envision contributing approximately 80 to 90 % of the troops, which would then be augmented by participation from a limited group of partners [46]. Finally, Security Force Assistance (SFA) largely comes down to helping, training, advising, and giving resources to partner countries characterised by regional instability, terrorism, or humanitarian crises to enable them to defend themselves and can take place in a wide variety of ways [6]. It can involve a handful of trainers being sent to an Allied country to train troops to large missions in which thousands of troops take part. The fact that these aspects are all developed in a NATO context shows that NATO recognises the importance of the comprehensive approach [42]. In addition, defence collaborations such as FNC and JEF show that NATO attaches great importance to cooperation between member states [46].

As far as the EU is concerned, it plays an important role in coordinating actions relating to the elimination of non-military threats [49]. Generally speaking, the EU aims to deepen and broaden EU integration [26]. In addition, and similarly to NATO, the EU also aims to increase the resilience of member states with respect to Eastern threats even if consensus achievement within the EU may be more difficult in this regard. From the perspective of member states, indications are that more importance is placed on the EU as an important tool in civil crisis management as compared to NATO where more emphasis is placed on military matters, [52]. Several noteworthy steps can be mentioned. First, the setting up of the European Defence Agency (EDA) in 2004 in order to promote greater cooperation in the industrial and development fields amongst EU Member States [26]. Second, with the Permanent Structured Cooperation (PESCO) in 2009, the EU was given a tool to connect the political aspects of European Defence to resources [45]. The Common Security and Defence Policy (CSDP) in turn allowed the EU to take a leading role in peacekeeping operations, in conflict prevention, and in strengthening international security [26]. Like NATO, the EU mainly relies on the capabilities of the Member States, which also limits its role to coordination. However, as the EU can rely on more than just military instruments unlike NATO, it may be better placed to pursue a diversified and comprehensive policy [11].

2.4.2.6 Bilateral and Multilateral Partners within International Collaborative Structures

Besides the International Organisations previously described, many countries enter ad hoc defence and security collaborations based on specific needs. At the very least, the partner countries can be considered as stakeholders but sometimes these initiatives acquire a distinct identity and lead to specific mechanisms. Many examples can be given such as the following ones mentioned in the final paper set:

- The Benelux defence cooperation between Belgium, the Netherlands and Luxembourg;
- The trilateral defence cooperation existing between Sweden, Norway, and Finland within the framework of the Nordic Defence Cooperation (NORDEFCO); and
- The Visegrad Group (V4) wherein Hungary, Poland, Slovakia, and the Czech Republic work together to achieve specific defence and security objectives.

First, building on the success of a previous naval initiative, new impetus for greater Benelux defence cooperation came in 2012 with the ‘Benelux Declaration on Defence Cooperation’ signed by the Ministers

of Defence of Belgium, the Netherlands and Luxembourg [10]. Within the Benelux framework joint planning, training, and procurement initiatives ensures greater cost efficiency and better resource utilisation within the three countries. The interoperability between the three countries is also strengthened, as is the coordination at the policy level [10]. Second, the Nordic Defence Cooperation (NORDEFCO) is centred on interoperability and the ability of the armed forces of two or more countries to train, practice and operate together in the execution of assigned missions and tasks. This cooperation is largely aimed at countering external aggression under a variety of manifestations [37]. Interestingly, Norway is a member of NATO, but Sweden and Finland are not. Third, the Visegrad or V4 group implies regional collaboration amongst the four following countries: Czech Republic, Slovakia, Poland, and Hungary. The aim of the cooperation is to coordinate in a variety of areas covering both military and non-military aspects including counterterrorism, cybersecurity, extremism, defence planning, energy security, common air policing, and crisis management [49].

2.4.2.7 Society or Population

The society or the population of a country traditionally plays a major but indirect role in influencing such things as policy, operations, and the capabilities that will be acquired by its own defence and security apparatus. Wallenius et al., go further by stating that it is desirable for the public to be familiar with the armed forces and their mission, as it must have confidence that the defence organisation operates in accordance with the missions defined by politicians and adequately reflects the values of civil society [53]. As will be discussed in the following sections, society's role as a stakeholder is different in every country, however. In some countries, the relationship is limited to the generation of general support and trust in order to be able to carry out standing mission and tasks. Still in others, the population plays a more direct and increasingly important role within frameworks such as Total Defence and Host Nation Support. Within the context of Total Defence for example, effective and active cooperation is required from the population, as a resource as such, but also in providing civilian infrastructure and civil support to the armed forces [54]. The same is stated with regard to Host Nation Support where, in the case of the Baltic States (Estonia, Latvia and Lithuania) for example, preparation of the necessary infrastructure to receive the partner countries is deemed to be the most important aspect besides the military one [49]. Indications are that a conflict or a visible threat may increase societal support for defence and security, as does the visibility an organisation is able to achieve through overseas deployments [53].

2.4.2.8 The Media

The media plays an important role in informing and spreading information about some of the previously mentioned stakeholders. This role of the media seems particularly important in light of some of the challenges that will be discussed in the "discussion" section such as a lack of trust that may exist between the population and the Government [41]. As epitomised by the concept of "strategic corporal", every decision and action taken by an organisation, even at the lowest level, can have a profound impact on the entire organisation, the policies it pursues, and the partners with which it collaborates [25]. By ensuing that decisions taken are directly subject to public scrutiny, the media, especially social media, has a major influence on how citizens perceive their security [41]. According to Mader's "Pretty Prudent Public Model", public support for a defence organisation is conditioned by the perception of objectives as explained by politicians and by the public's own assessment as to the effectiveness and the legitimacy of military activities [33]. It follows that both politicians and the defence and security apparatus need to adequately focus on strategic communication and their relationships with media organisations. For the defence and security apparatus specifically, this means that visibility and the demonstration of performance, accountability and transparency is paramount [19].

2.4.2.9 Crisis Management Actors and First Responders

Within the framework of crisis management, a number of stakeholders can be identified on which the defence and security organisations depend on if called upon as a last resort. These actors include specific

military units tasked with crisis response, first responders (such as the Police, the Fire Brigade, Civil Protection, hospitals, and NGO's), and local authorities (Local Government, Provincial Government or Regional Government depending on the magnitude of the crisis). Within the final paper set the following examples can be given:

- The "Secrétariat Général de la Défense Nationale" (SGDN, FR);
- The "Unidad Miltar De Emergencias" (UME, SP); and
- The Ministry of Justice and Police (NOR).

First the "Secrétariat Général de la Défense Nationale" can be identified as the main stakeholder of the French Defence regarding crisis management [55]. This inter-ministerial body aims to assist the Prime Minister in the various facets that may jeopardise the country's security. It does so by evaluating the risks and threats and ensuring that plans are coordinated. Second, in Spain, the "Unidad Miltar De Emergencias" operates in the civilian sector but is part of the armed forces. Its aim is to intervene anywhere in the country where the safety of civilians is at risk in synergy with the other public services. Third, in Norway, the Ministry of Justice and Police has an important responsibility in preparing for emergencies and coordinating responses in case of crisis situations [55].

Besides the fact that each nation has its specificities, several general observations can be made. First, there is a general expectation that Defence should provide assistance when civilian resources are not sufficient and upon the specific request of civilian authorities. As such, the actions carried out by the military organisation must be justified and integrated into civilian operations. Second, in many countries (such as Italy, Spain and Norway), CBRN capabilities, as opposed to other response and rescue capabilities, may be an area where expertise mostly lies within the Defence department.

2.4.2.10 Intelligence Services

The information retrieved on intelligence services was limited and vague; probably due to classification issues, which is also a consideration of this study. Therefore, even if we will not dwell extensively on the role and tasks of the intelligence services, it can be established that these partners play important roles given current security challenges. Tasks of the intelligence agencies identified included combatting (global) terrorism, threat identification, support to planning of operations, carrying out of reconnaissance, intelligence gathering and ensuring state security [7], [8]. The literature also points to the workings of intelligence services in the cyber domain. Gathering information on enemy activities allows one to better develop one's own cyber techniques and resources so that they be more effective and better prepared for times of crisis [7], [31] .

2.4.2.11 Cyber Agencies

The enhanced focus on the cyber aspect nowadays, and the enhanced level of cooperation required from defence and security organisations in this domain, has often led to the establishment of distinct agencies for this purpose [7]. Within the final paper set, examples include the:

- Government Communications Headquarters (GCHQ, UK);
- National Cyber Security Centre (NCSC, UK); and
- Cooperative Cyber Defence Centre of Excellence (CCDCE, NATO).

First, the GCHQ is responsible for monitoring cyber threats across the United Kingdom, doing so for approximately 450 companies in numerous sectors such as aviation, defence, energy, transport, and telecommunications and thereby acting as the UK's cyber expertise centre [31]. In turn, the NCSC was established in 2016 and falls under the GCHQ. Its specific aim is to unify cybersecurity expertise and capabilities which were previously dispersed in other institutions and to be the leading UK authority in

the field of data security and information sharing [31]. Last, the CCDE's mission is to enhance the capability, cooperation and information sharing among NATO, its Member States and Partners by virtue of education, research and development, lessons learned and consultation [40]. Like for the intelligence agencies, we will not delve further into cyber aspects. However, it can generally be said that these capabilities may be used defensively and offensively, in peacetime and in war. In addition, laws and regulations on this subject are often ill defined in international law making them open to interpretation and creating a grey zone in which it is not clear what is or is not allowed [7].

2.4.2.12 Private Companies

Defence organisations have also always had a link with the industry in order to maintain technological parity or superiority. Accordingly, within the final paper set, several big research and capability development programs were identified with the main partners being the leading country and the companies involved. Within such big programs, there is most often a desire if not a need to cooperate and to export to partner countries to reduce the costs of manufacturing and purchasing. For example, in the case of the Tempest program, the leading country is the UK, and the industry partners include BAE Systems, Leonardo, MBDA and Rolls Royce [32]. For the private companies, the main objective is profit even if other objectives such as market share and employment are sometimes relevant. For the leading country, a big program on the scale of Tempest allows it to preserve its industrial and technology base [19], [32].

Defence and security organisations are also increasingly looking at the possibility of outsourcing due to declining defence budgets and the need to work in a cost-efficient way. The other big expectation of defence organisations is that PMSC will be able to fill a lack of manpower especially with respect to technology-intensive functions. By outsourcing such aspects, defence organisations expect to be able to better focus on their core business [17]. Usually, services from the civilian sector are sought that can take over specific capabilities [17]. However, outsourcing is increasingly not limited to support functions with core security tasks also being increasingly carried out by Private Security and Military Companies (PMSC) including in such domains as logistics, recruitment, and surveillance [5]. Interestingly, NATO states that about 90% of military transport is borrowed from the private sector and that it depends on commercial companies for about 50% of satellite communications [54]. Similarly, within the framework of Host Nation Support, about 75% of the support to NATO operations comes from local civilian services and infrastructures [54]. The PMSC's see such cooperation in a positive light. Besides the opportunity to making a profit, they see it as an opportunity to easily recruit highly qualified military personnel as well as an opportunity to increase their legitimacy [5].

2.4.2.13 Personnel

Personnel play a critical role in fostering cooperation as well with evidence that sometimes they have provided the impetus for cooperation in the absence of top-down will or initiatives [1], [43]. In the literature, the role of civilians working within a defence organisation is emphasised within this context. Although they perform a large range of tasks (ranging from highly specialised to relatively unskilled work) and are usually tasked with activities that are not part of core military work, they bring non-military expertise and continuity to the organisation [1], [25]. According to Egnell, they do not only offer better insights into public finance or diplomacy, but also have the ability to work closely with representatives of other government departments [15]. Notably, they can be occupying key positions such as advising ministers on strategy and the political and economic impact of plans [25]. Still according to Egnell, greater integration of civilians and military leads to better advice on political matters, better knowledge of military matters within ministries, and better understanding of political concerns within the military hierarchy [15]. Second, without military personnel, a defence organisation cannot achieve any objective. In addition to defence and security personnel working in the aforementioned structures, civilian or military, immediate family members and communities may also be considered as stakeholders [12].

2.4.2.14 Humanitarian, Development Cooperation and Non-Governmental Organisations

A lot can be found in the literature about diverse humanitarian actors. In the context of this research, they have all been placed under the same category, however. Defence and security organisations encounter these humanitarian or development cooperation organisations during and after conflicts [2], [16]. Although not every NGO carries out the same tasks, providing resources, providing medical assistance, providing food and water, providing education, providing sanitation, and building the necessary infrastructure can be stated to be amongst the most common ones [2]. A number of examples are cited in the final paper set with "Médecin Sans Frontières" (MSF), World Health Organisation (WHO) and International Committee of the Red Cross (ICRC) being the most prominent examples.

Defence organisations may see a number of advantages in collaborating with humanitarian organisations. According to Malešič, defence organisations may see this as a way to polish their public image [34]. On the other hand, most humanitarian stakeholders adhere to the principles of humanity, impartiality, neutrality, and independence. In doing so, they attempt to distinguish themselves from any politically motivated activity and may therefore be weary of collaborating with defence organisations [16]. Despite intervening and operating on different principles however, partners need to be able to work well together as they influence each other' functioning and the achievement of each other's objectives. Therefore, despite the fear for association with military activity, many humanitarian actors accept that the military organisation can play a legitimate and vital role in humanitarian operations [34]. Some recognise the usefulness of the unique transport possibilities that a defence organisation can offer [2]. One line of thought put forward is that humanitarian and defence organisations need to work more strategically (for example during planning phases) in order to avoid potential risks associated with civil-military cooperation while at the same time enhancing mutual benefits [34]. Apart from the struggles that exist, both have the same objective in mind: To alleviate pain and suffering and prevent fatalities [2]. In other words, the political goals may often be the same even if the tools to achieve these goals may be very different.

2.4.3 Comprehensive Defence Frameworks: Identification, Benefits and Limitations

Our research did not identify a single framework or model within which all the aforementioned stakeholders were represented. Therefore, in the following section, we present the different frameworks and models identified wherein some of the stakeholders pertaining to collaboration between defence and security organisations are present. Since most of these frameworks have already been discussed in some way in the previous section, they will only be discussed briefly.

2.4.3.1 Defence Diplomacy and Development (3D) and its Variants

There are several versions of the 3D approach mentioned in the literature, but the three core departments remain the same. The Ministry of Foreign Affairs usually takes the leading role in this format of cooperation whereas the Department for Development Cooperation usually has a subordinate role as it often falls under the Ministry of Foreign Affairs [27]. This is for example the case with the Dutch Department for Development Cooperation and the American United States Agency for International Development. In the United Kingdom however, the Department for International Development seems to take a more prominent role as it is responsible for the Stabilisation Unit created to coordinate interdepartmental cooperation. The British version is also extendable as it indicates that one may move from a 3D approach to a whole-of-government approach encompassing economic and justice components. Interestingly, all the different versions of 3D have in common the fact that they are primarily aimed at tackling crisis situations in fragile states [52].

2.4.3.2 Whole-of-Government

According to the American version of this concept, the whole-of-government concept consists of a 3D approach coupled with an on-site whole-of-government approach. As such, the whole-of-government

approach is therefore broader than the 3D approach because it includes not only the three different national government departments of the intervening or donor country but also the institutions of the fragile state or recipient country which it benefits [27]. In the American mind-set, there is also talk of a whole-of-alliance approach where the importance of national institutions working together with allied partner countries is highlighted.

2.4.3.3 Integrated Approach

When a whole-of-government approach is extended to the formation of joint and integrated structures, mostly within the context of complex expeditionary operations, an integrated approach is implied. According to Egnell, such structures offer multiple benefits [16]. First, unity of command and effort offer the best opportunity to successfully complete assignments. Second, integrated structures may also provide accurate and adapted information to the various organisations involved, thereby ensuring that the organisations involved are better adapted to the strategic context. Third, the existence of integrated command and control structures at the strategic level enables relevant stakeholders to coordinate during the planning and implementation of actions. The literature also shows that an integrated approach can be much broader than just complex operations. For example, the UN and the EU more often than not refer to an integrated approach rather than a comprehensive approach [52].

2.4.3.4 Total Defence

Total Defence is a whole-of-society approach that seeks to deter a potential enemy by increasing the cost of aggression and reducing the chances of success [54]. It takes both military and civilian aspects into account generating extensive cooperation between the Department of defence, other Ministries, civil society organisations, the private sector and the general public [52], [54]. This can be seen very broadly as ‘social resilience” to include such concerns as a healthy economy to a low degree of corruption [46], [54]. Also, what is important within this framework is the ability of a country and the population to rely on itself in an autonomous way in withstanding any aggression. Two terms that are often cited here are resilience and territorial or homeland defence. Resilience can be seen as society’s ability to resist and recover from crisis situations in which there must be a combination of civil, economic, commercial, and military factors [54]. This seems to be highly relevant in the contemporary context of hybrid threats arising from the East attacking any country’s weaknesses and fragility [52]. The military aspect of Total Defence is territorial defence. Here, the military organisation will enjoy extensive support from the civil sector and adopt a rather defensive attitude in which a potential aggressor will be discouraged by denying access to the territory [54].

In the literature, this concept was mainly found in the following countries: Finland, Sweden, and Norway with the Nordic Defence Cooperation (NORDEFCO) providing support for cooperation amongst the mentioned countries. Finland is often seen as a model for Total Defence as far as it has always maintained its comprehensive defence approach and underlying capabilities even after the end of the cold war. This makes it the better prepared country, especially with regard to the mobilisation of the Finnish population [54]. Still according to Wither, Norway seems to have the most complete and comprehensive Total Defence manual. Here the focus is to use society’s limited resources in the best possible way in times of crisis [54].

While the Nordic countries have been working on this concept for some time, as they are confronted with an active threat from the East, the concept may not be well known in other countries. However, it can certainly be interesting for other EU and NATO countries to study the concept more closely especially within the context of hybrid threats [52]. According to Wither, the Nordic countries have some advantages over NATO and EU partner countries as they do not suffer from weak governance, vulnerable institutions, large ethnic minorities, corruption, and low public confidence which are precisely the aspects that make a country vulnerable [54]. It is therefore not yet clear if such a concept is also applicable in contexts where there is no history or culture of extensive cooperation between military and civilian services [52]. It is also not yet clear

if the concept is applicable within countries that have populations that are highly divided along ethnic, religious and linguistics lines. This is because Total Defence remains dependent on the will of the population to defend the country: it is asked to make a huge effort in peacetime and must show tremendous resilience and resistance in wartime [54].

2.4.3.5 Crisis Management, Emergency Management and Disaster Management

While each country usually has its own framework and mechanisms in the field of crisis management, some generic observations can be made, however. First, the National (or Federal) Government usually takes the political decisions concerning the objectives and framework for disaster preparedness and crisis management. Second, there is often a dual structure: a national decision-making body containing the relevant Ministers and the Head of Government as well as one or more coordinating bodies where their representatives operate and further implement decisions. Third, the management of an actual crisis is usually carried out at the level best corresponding to the size and the nature of the event. Generally, following a logic of proximity or subsidiarity, this means that crises are tackled at the lowest possible level. Fourth, overall responsibility is usually handed to the organisation responsible for providing the service during normal situations. In line with this principle, each Ministry or Agency is responsible for planning, training, and implementing crises-response actions within its area of responsibility. Fifth, a crisis plan is usually mandated containing such items as risk analysis and planning for emergency measures. Finally, usual threats identified in this context include chemical, biological, radiological, nuclear, flood response, terrorist attacks and industrial disasters.

2.5 DISCUSSION

2.5.1 Legal Framework for Cooperation between Stakeholders

Along with the cooperation structure and the underlying power bases, the legal framework is also an important parameter characterising cooperation between stakeholders. There are a diverse set of options, but a few broad categories were identified, which are more or less presented in a hierarchical order from a legal standpoint.

First, within the context of international organisations one can identify treaties forming the basis for the creation and the operations of some organisations. For example, the most important treaty within NATO remains the Washington Treaty [7]. Another example is the establishment of PESCO in 2009 within the purview of the Lisbon Treaty [45] Next to treaties, countries may opt for international declarations and agreements either sub-ordinated to a higher order treaty, as an annexed protocol, or as a stand-alone. A good example of a stand-alone agreement found in the literature is the NORDEFCO cooperation initiative in 2009 regrouping previous agreements between the three Nordic countries under a single framework [37]. In turn, international bodies may themselves develop strategies and guidelines that affect collaboration amongst the member states. For example, in 2013, the EU published the Cyber Security Strategy of the European Union [11].

Further, most countries engaging in international collaboration integrate at least some aspects into national legal texts. This certainly comes to the fore in the context of Total Defence and Host Nation Support. For example, within the HNS context adjustments were made to the national Lithuanian laws in 2011 so that the restrictions on the number of allied troops on the territory and the access of warships to Lithuanian ports were lifted [42]. In the context of civil-military crisis management, responsibilities for emergency situations are also often laid down in national laws. For example, in Italy a decree of 1999 gives responsibility for civil protection (Fire Brigade, Civil Protection, etc.) to the Ministry of the Interior. Still within the context of crisis management, the national laws often lead to national plans being drawn up. For example, in France, numerous plans have been drawn up to combat chemical and biological terrorism including the PIRATOX plan against chemical terrorism, the BIOTOX plan against biological terrorism and the PIRATOM plan against radiological terrorism [55].

Next to the documents originating from the parliamentary level, documents may also originate from the governmental level in diverse forms and formats including national strategy papers, Memorandums Of Understanding (MOU) and Letters Of Intent (LOI). Higher order national strategy papers may be important to overcome some of the organisational barriers hindering cooperation such as a lack of incentive or lack of common budget, [52]. For example, in 2006 a National Security Strategy was issued in the USA where the emphasis was placed on improving the 3D approach [27]. For the UK, the Building Stability Overseas Strategy of July 2011 can be mentioned [28]. Still, in Finland, there is such a thing as the Security Strategy for Society, which contains guidelines for cooperation to safeguard the most important societal functions [54]. As far as MOU's are concerned, an example is the bilateral memorandum of understanding signed by Finland and Sweden called Air Picture Exchange regarding the exchange of air surveillance information in 2017 [37] Last, Letters Of Intent (LOI) seem to be more oriented towards big military projects and outsourcing along with classic contracts. For example, the Swedish Army and two PMSCs singed an LOI in 2017 attempting to shape career opportunities for military personnel after their time in the army [5].

Interestingly, the literature also identifies legal gaps and grey areas in the field. One such gap is the lack of clear guidelines defining collaboration between security and humanitarian actors in the field of development cooperation. Ad hoc procedures, informal contacts, and cultural empathy are therefore required to maintain relationships in such cases [35]. Yet another gap is the absence of rules relating to support to civil authorities following large-scale cyber-attacks [7]. One ambiguous area is for example the fact that NATO doctrine makes no mention of how Host Nation Support is to be conducted in wartime [42]. This is also the case of NORDEFCO in the sense that it only regulates cooperation in peacetime [37]. Like the field in general, the legal framework regulating it also indicates still developing maturity [7].

2.5.2 Challenges and Factors Affecting Cooperation between Stakeholders

In such a diverse field, there are obviously many challenges some of which are relatively complex. First, complexity arises from the fact that the relationships between actors in any comprehensive national defence framework are hardly linear, dyadic, or simple. Actors also influence each other indirectly and constantly through third parties. For example, the perception and relationship between society and the defence organisation is shaped and influenced by politicians and the media [33].

Second, a difference in vision, goals, interests, and objectives can undermine any collaboration. At the policy level, the Government and the defence organisation may not always be on the same wavelength. There is not always a common understanding of how strategy should be conducted [25]. Whereas military personnel mainly focus on the objective to be achieved, politicians mainly look at the most important things that need to be done first [53]. Also, the military usually wants policy decisions to be taken as quickly as possible so that maximum time remains for planning, whereas politicians usually prefer to postpone decisions as long as possible so that all options remain on the table [25]. Likewise, in the field of interdepartmental cooperation, differences in time perception seems an important challenge that needs to be overcome. For example, Foreign Affairs and the Defence tend to have a short-term vision in responding to crises, whereas Development Cooperation tends to have a long-term vision to realise long-term projects [27]. Similarly, an important aspect in entering into a defence collaboration such as NORDEFCO or Visegrad is whether the countries share common priorities and have a common threat perception [49], [54]. A corollary question is how much sovereignty countries are willing to forgo. Even in groups where countries belong to the same region and have similar strategic objectives, it is difficult to reach consensus [49]. This problem is also highlighted by Küsters in the context of big industrial projects where countries do not always share the same vision about the functionality or design of the system [26]. In addition, each industrial partner has his own priorities and objectives that may also influence the cooperation [32].

Third, cultural differences and a lack of knowledge can have a major impact. Whereas a common language seems essential, so that everything remains intelligible to all parties, this is not always the case [27]. As such, differences in values and culture seem to be major factors negatively influencing cooperation in the fields

of development cooperation and collaboration with private companies [5], [28]. On the other hand, cultural similarity may be a positive factor enhancing cooperation between Nordic countries [37]. A lack of knowledge that stakeholders may have on each other may also negatively affect relationships. According to Kiszely, politicians and military organisations lack knowledge about each other's operations and culture and find it difficult to put themselves in each other's shoes [25]. According to Wallenius et al., the knowledge society has about the defence organisations is deficient and influences the importance and support it gives to the organisation [53]. Still according to Apte et al., lack of knowledge about each other's resources, organisation structure, and competencies leads to duplication of effort and inefficiencies [2].

Fourth, budget, its utilisation, or the lack thereof can have a major influence between defence organisations and stakeholders affecting cooperation in various ways. For example, according to Cornille, only 0.3% of the member states' budget is used to jointly finance projects within the framework of NATO [11]. Where countries provide more than 95% of the capabilities, NATO mechanisms bear much responsibility for the elements that are needed to improve coordination and interaction between Member States. High costs, decreasing budgets and enhanced focus on burden sharing encourage countries to cooperate more however [26], [32], [46], [49], as in the context of joint capability development, FNC initiatives, and big industrial projects. Declining budgets also encourages more outsourcing and collaboration with PMSC's [17].

2.5.3 Managerial Implications

There are a number of options that can make cooperation between stakeholders and the defence organisation more efficient. Some of the most important management options identified are now discussed.

First, in the literature it appears frequently that a common budget can promote cooperation, especially in the context of interdepartmental and defence cooperation. Several examples are given with the UK and the Netherlands having the most compelling examples of a common budget for their interdepartmental cooperation. In the UK, since 2015, this budget is called the Conflict Stability and Security Fund and is placed under the purview of the UK National Security Council. In the Netherlands, since 2012, it is called the Stability Fund and is placed under the purview of a ministerial committee consisting of Foreign Affairs and the Ministry of Defence [27], [28]. Other examples mentioned in the literature include the European Defence Fund, a V4 fund to support scholarships between participant countries called the International Visegrad Fund [49] and the NATO Security Investment Programme by NATO and the USA to improve cooperation within the framework of Host Nation Support in the Baltics [42].

Second, permanent coordination structures and fora with a strong mandate ensure better coordination and communication [15]. The existence of the Stabilisation Unit within the British interdepartmental cooperation can be highlighted. By focussing on the identification and definition of policy items, and on the planning and analysis level, it allows the UK to have a coordinated policy on humanitarian, political, military and development cooperation aspects across multiple departments [15], [27], [28]. According to Egnell, such fora are also important at the higher political level in order to provide permanent dialogue, consensus, and advice mechanisms between top military and civilian leadership [15]. Again, the British Government is said to provide the good example with its system consisting of the Cabinet and underlying ad hoc committees [15]. Interestingly similar structures of steering committees also exist in the Netherlands such as the "Fragility and Peacebuilding Unit", the "Military Operations Steering Group'' and the "Police/Rule of Law Steering Group" [27]. Further, joint tools for threat analysis, situational awareness, determination of requirements and planning across departments may also foster common vision and cooperation. In the Netherlands, for example, the geographical analysis offices are synchronised between the various departments [2], [27].

A third important point is the enhancement of knowledge management and information exchange. One tool to enhance cooperation is the exchange of advisors or liaison officers. Mostly this happens within the context of interdepartmental cooperation or international cooperation. Notably, and even if the added

value is contested, Sweden has a programme in which officers from the Swedish Army work for a PMSC for a certain period before being said to return with valuable knowledge for the Swedish Army [5]. A second tool is the creation of common communication networks to quickly share classified information amongst partners [37]. A third tool that can be used in this regard is a 'lessons learned' database. Interestingly, one is present in the Netherlands within the Department of Development Cooperation and the Ministry of Defence as well as within the UK Stabilisation Unit [27]. Fourth, perhaps one of the most important options is the existence of common training courses and exercises. For example, within the previously mentioned Dutch Task Forces, there are experts from the Department of Development Cooperation and the Ministry of Defence who regularly organise joint exercises in order to better anticipate each other's working methods [27]. Many other examples can be provided including the exercises taking place as part of the trilateral cooperation between Norway, Sweden and Finland [37], the 'Baltic Host' exercises organised by the Baltic States [42], and the yearly large-scale exercise organised by the Visegrad group [49]. These exercises provide many benefits. Amongst other, they ensure that stakeholders are interoperable and able to work together. They also allow evaluation of particular capabilities such as whether Host Nation Support related ones are sufficient [37], [42]. At the strategic politico-military policy level, the importance of this aspect is also recognised. If both political and civil leaders were to take part in the same courses and exercises together, the mutual knowledge about each other could be increased [25]. Finally, the use of a single common language such as English enhances cooperation and interoperability [37].

Fourth, the importance of strategic communication in demonstrating the need for the existence of the organisation as well as the added value it provides to the most important stakeholders cannot be over-emphasised [53]. The stakeholders need to be informed about the policies and the most important objectives that the organisation wishes to achieve [30]. Demonstrating transparency, accountability and effectiveness is important to create trust between the defence and security apparatus and some of the more important stakeholders such as politicians and the population [44]. In this regard, offering support in times of national crises is an opportunity to enhance organisational visibility with respect to society [53]. In order to achieve positive effects, there is a need for communication tools as well as the need for planning and executing coordinated communication and messaging campaigns. A good plan must have measurable objectives and makes it possible to reduce the positive or negative influence of the media [44]. Not only the impact on the target audience is important, but stakeholders' perceptions of the organisation can be used to adjust policy and objectives [30], [44].

2.6 CONCLUSION

In this study, our main objective was to provide an overview on the vast and rapidly developing field of comprehensive approach and comprehensive national defence systems. For this purpose, a Systematic Literature Review (SLR) was conducted using a six-phased process adapted from Higgins et al., [21] and Tranfield et al., [48] on three platforms being Scopus, the NATO Library and SharePoint. The search was executed based on title, keywords and abstract in Scopus and an equivalent technique on the other two platforms. Consequent to the broad search strategy and search terms, we identified 10121 unique results in Scopus, 1051 unique results in the NATO library, and an unknown number of results in SharePoint. Our initial review based on the title and abstract of each paper narrowed the results to 631 papers from Scopus, 23 papers from the NATO platform and 85 results from SharePoint that were deemed relevant or potentially relevant. In the second and final review process, a total of 739 available documents were therefore analysed based on a review of the full paper content. Ultimately, 147 papers were retained to which seven documents directly obtained from NATO SME's was also injected to constitute the final paper set of 154 papers (see Appendix 2-1). The bibliometrics of this final paper set was done using several tools such as Scopus analytics, MS Excel, Mendeley and VOS Viewer. Data extraction was based on the research questions and performed in two MS Excel and MS Word simultaneously.

Amongst the bibliometric results, we established that the top ten journals in the field seemed to be Defence Studies, Defence and Security Analysis, Disaster Medicine and Public Health Preparedness, Small Wars and Insurgencies, the International Journal of Emergency Management, Armed Forces and Society, the Journal of International Peacekeeping, International Peacekeeping, the Journal of Humanitarian Logistics and Supply Chain Management, and the Journal of Strategic Studies. In doing so, the final paper set seemed to originate from journals more focused on defence, emergency, and strategy. Based on impact factor considerations, we further refined the top journals for submission to be the Journal of Humanitarian Logistics and Supply Chain Management, followed by International Peacekeeping, Small Wars and Insurgencies and the Journal of Strategic Studies. As far as authors are concerned, it appeared that 25 authors had two or more publications in the final paper set, out of which twelve authors seemed to focus on the topic only. Three clusters of authors were also identified which were all connected by at least one author. Further, the results also indicated that the USA and the Netherlands are probably the countries being missed the most in the RTG due to which they may be specific targets for inclusion in future initiatives. Overall based on several indicators [24], we considered the research area to be at a low but still developing level of maturity.

Besides being the first SLR and bibliometric analysis identified in the field of CA, our study also provided insights on contemporary issues in the field. Accordingly, we identified the main stakeholders of defence organisations as being Ministries (such as Foreign Affairs and International Aid), politicians (such as Heads of Government, Ministers, the Government, and Party leaders), national coordinating bodies (such as National Security Councils), International organisations (such as NATO and the EU), bilateral and multilateral partners, one's own society or population, the media, crisis management actors (such as the Police and Civil Protection), intelligence agencies, cyber agencies, humanitarian organisations (such as the ICRC) and private companies. Although we were not able to identify a single comprehensive approach framework incorporating all these different stakeholders, we identified 3D (Defence, Diplomacy and Development), its variants, the Whole-of-Government approach, the Integrated approach, Total Defence, and the national crisis management systems as being the most prominent frameworks relating to the topic. While the Integrated approach seems to be the most far reaching form of collaboration in the field of complex expeditionary operations, Total Defence seems to be the most far reaching in terms of defence of the homeland and resilience.

Identifying stakeholders and linking them with some of the previously mentioned CA frameworks should enlighten us as to the approaches used and their comprehensiveness within various countries. In addition, by summarising the legal architecture in the field, discussing some of the most commonly identified challenges, identifying some of the most important managerial implications, and establishing some avenues for further research, our study provides SMEs with a strategic platform to further engage on the subject. Thereby, this study contributes towards the further development of the CA concept within the defence and security realm.

2.7 LIMITATIONS AND FUTURE PERSPECTIVES

Carrying out an SLR entails restrictions by design, and strategy choices have to be made, thereby also opening up opportunities for further research. First, since, the results may vary depending on the platform chosen, it is always possible to broaden or explore other platforms. Rudimentary testing on Web of Science indicates that the nature of the trends previously desired would not vary much but other type of platforms such as ProQuest and Ebscohost may indicate otherwise. Second, the search results were constrained as from 2005 to prioritise modern developments in the field but discussions with SME's indicate that it may be insightful to also study predating seminal papers as well. Third, when drawing and executing the search strategy in a pre-COVID world, subject areas such as immunology and terms such as virus were filtered out from the results. In view of the COVID pandemic, it may be interesting not to omit this filter for future research, as this can undoubtedly provide valuable results as indicated by preliminary discussions outside and inside the RTG.

As far as the synthesis is concerned, given the number and the diversity of the results obtained in phase five, a large number of papers are available for more focused future research. For example, only papers touching on Total Defence or cyber defence may be studied. Alternatively, only papers exploring the strategic level of defence organisations could be studied. Future endeavours may also attempt to enlarge the definition a stakeholder to also consider negative influencers as this may generate valuable, possibly different, and complimentary results.

Finally, yet importantly, as the focus of this study was purely literary and academic, national case studies generating practical and real-world insights would be interesting and a logical complementary step. As nations evaluate the state of play of their CA initiatives with each other and with the literature, future perspectives of international collaboration on comprehensive defence could be instigated. Case studies would also allow generalizations to be drawn amongst nations and comparisons to be made between the theory and practice thereby further contributing to the maturity development of the research area.

2.8 ACKNOWLEDGEMENTS

First, we would like to thank those NATO national representatives who provided additional documents to complement the literature review results. Second, we would like to thank Mr. William Demeyere who developed parts of the overall study within the context of his master thesis thereby facilitating the generation of some of the results and insights. Finally, we acknowledge funding from the Royal High Institute for Defence (Belgium).

2.9 REFERENCES

[1] Andres, M., and Soeters, J.M.L.M. (2015), "Werkrelaties tussen militairen en burgerpersoneel bij Defensie", Militaire Spectator: Tijdschrift voor het Nederlandsche Leger, Vol. 184 No. 9, pp. 374-387.

[2] Apte, A., Gonçalves, P. and Yoho, K. (2016), "Capabilities and competencies in humanitarian operations", Journal of Humanitarian Logistics and Supply Chain Management, Vol. 6 No. 2, pp. 240-258.

[3] Archuleta, B.J. (2016), "Rediscovering defence policy: A public policy call to arms", Policy Studies Journal, Vol. 44 No. S1, pp. S50-S69.

[4] Bergman, E.M.L. (2012), "Finding citations to social work literature: The relative benefits of using Web of Science, Scopus, or Google Scholar", The Journal of Academic Librarianship, Vol. 38 No. 6, pp. 370-379.

[5] Berndtsson, J. (2019), "The market and the military profession: competition and change in the case of Sweden", Defence and Security Analysis, Vol. 35 No.2, pp. 190-210.

[6] Biddle, S., Macdonald, J., and Baker, R. (2018), "Small footprint, small payoff: The military effectiveness of security force assistance", Journal of Strategic Studies, Vol. 41 No.1-2, pp. 89-142.

[7] Bigelow, B. (2019), "What are Military Cyberspace Operations Other Than War?", in Cyber Conflict 2019 proceedings of the 11th International IEEE Conference, Vol. 900, pp. 1-17.

[8] Bruneau, T.C. (2018), "A conceptual framework for the analysis of civil-military relations and intelligence", Defence and Security Analysis, Vol. 34 No. 4, pp. 345-364.

[9] Bryson, J.M. (2004), "What to do when stakeholders matter: stakeholder identification and analysis techniques", Public Management Review, Vol. 6 No. 1, pp. 21-53.

[10] Coelmont, J. and Badot-Bertrand, H. (2019), "Interveiws of Thys, M., Matthijssen, K. and Kalmes, Y. for the Belgian Military Publication", Royal Higher Instiitute for Defence, Brussels, Belgium.

[11] Cornille, L. (2014) "Inzet van cybercapaciteiten", Koninklijke Militaire School, Brussels, Belgium.

[12] Daems, I. (2014), "Pre-, during, and post-deployment psychological care for soldiers and their families in the Austrian and Belgian Armed Forces", Royal Military Academy, Brussels, Belgium.

[13] Decraene, C. (2017), "Het concept 'fragiliteit' bij de planning en uitvoering van Belgische militaire operaties in het kader van een interdepartementale samenwerking, Koninkelijke Militaire School, Brussels, Belgium.

[14] De Kerchove, G., and Höhn, C. (2013), "Counter-terrorism and international law since 9/11, including in the EU-US context", Yearbook of International Humanitarian Law, Vol. 16, pp. 267-295.

[15] Egnell, R. (2006), "Explaining US and British performance in complex expeditionary operations: The civil-military dimension", journal of strategic studies, Vol. 29 No. 6, pp. 1041-1075.

[16] Egnell, R. (2013), "Civil–military coordination for operational effectiveness: Towards a measured approach", Small Wars and Insurgencies, Vol. 24 No. 2, pp. 237-256.

[17] Erbel, M. (2017), "The underlying causes of military outsourcing in the USA and UK: bridging the persistent gap between ends, ways and means since the beginning of the Cold War", Defence Studies, Vol. 17 No. 2, pp. 135-155.

[18] Freeman, R. (1984), "Strategic management: A stakeholder approach", Boston: Pitman, Vol. 46.

[19] Garbers, F., Glaerum, S., Haynes, C., Lacire, R., Lawrence, A., Letens, G., ... and Young, C. (2020), "Performance management in defence organisations", Science and Technology Organisation, North Atlantic Treaty Organisation, Neuilly-sur-Seine, France.

[20] Harzing, A.W., and Alakangas, S. (2016), "Google Scholar, Scopus and the Web of Science: A longitudinal and cross-disciplinary comparison", Scientometrics, Vol. 106 No. 2, pp. 787-804.

[21] Higgins, J.P., Thomas, J., Chandler, J., Cumpston, M., Li, T., Page, M.J., and Welch, V.A. (Eds.), (2019), Cochrane handbook for systematic reviews of interventions, John Wiley and Sons.

[22] Johnson, G., and Scholes, K. (2002), "Exploring corporate strategy", Sixth Edition, Pearson Education, Harlow, England.

[23] Keathley, H. (2016), "The systematic literature review process", University of Central Florida", Orlando, Florida, United States of America.

[24] Keathley-Herring, H., Van Aken, E., Gonzalez-Aleu, F., Deschamps, F., Letens, G., and Orlandini, P.C. (2016), "Assessing the maturity of a research area: Bibliometric review and proposed framework. Scientometrics", Vol. 109 No. 2, pp. 927-951.

[25] Kiszely, J. (2019), "The political-military dynamic in the conduct of strategy", Journal of Strategic Studies, Vol. 42 No. 2, pp. 235-258.

[26] Küsters, C. (2018), "Why is there no joint European remotely piloted aircraft system project under the common security and defence policy?", The RUSI Journal, Vol. 163 No. 2, pp. 52-65.

[27] L'Evêque, G. (2017). "Defence, diplomacy and development: The Belgian approach", Royal Military Academy. Brussels, Belgium.

[28] Leclercq, S., Klimis, E., Matagne, G., Martini, J., and Vervisch, T. (2018), "A comprehensive approach for Belgian Development Cooperation", Evidence Paper Series, 2018/002.

[29] Levy, Y. (2013), "How military recruitment affects collective action and its outcomes", International Studies Quarterly, Vol. 57 No. 1, pp. 28-40.

[30] Lim, Y.J. (2015), "Theorizing strategic communication in parsimony from the U.S. government perspective", KOME − An International Journal of Pure Communication Inquiry, Vol 3 No.1, pp. 1-15.

[31] Lonsdale, D.J. (2016), "Britain's emerging cyber-strategy", The RUSI Journal, Vol.161 No. 4, pp. 52-62.

[32] Louth, J., and Spragg, A. (2019), "UK future combat air: A programme management imperative", "The RUSI Journal", Vol. 164 No. 4, pp. 46-59.

[33] Mader, M. (2017), "Citizens' perceptions of policy objectives and support for military action: Looking for prudence in Germany", Journal of Conflict Resolution, Vol. 61 No. 6, pp. 1290-1314.

[34] Malešič, M. (2015), "The impact of military engagement in disaster management on civil-military relations", Current Sociology, Vol. 63 No. 7, pp. 980-998.

[35] McConnon, E. (2018), "The security-development nexus in Ireland's foreign policy: Challenges and opportunities", Irish Studies in International Affairs, Vol. 29, pp. 119-132.

[36] Mitchell, R.K., Agle, B.R., and Wood, D.J. (1997), "Toward a theory of stakeholder identification and salience: defining the principle of who and what really counts", Academy of Management Review, Vol. 22 No.4, pp. 853-886.

[37] Møller, J.E., (2019), "Trilateral defence cooperation in the North: An assessment of interoperability between Norway, Sweden and Finland", Defence Studies, Vol. 19 No. 3, pp.235-256.

[38] Muñoz, J.A. M., Viedma, E.H., Espejo, A.L.S., and Cobo, M.J. (2020), "Software tools for conducting bibliometric analysis in science: An up-to-date review", El Profesional de la Información, Vol. 29 No. 1, e290103.

[39] NATO (2003), "NATO civil-military co-operation doctrine", STANAG2509/AJP-9.

[40] NATO CCDCOE (2019). "Expertise and cooperation make our cyber space safer", e-Estonia,16 October 2018, Retrieved 29 August 2019.

[41] Norri-Sederholm, T., Elisa, N., Aki-Mauri, H. and Karoliina, T. (2019), "Social media as the pulse of national security threats: A framework for studying how social media influences young people's safety and security situation picture", In Proceedings of the 6th European Conference on Social Media, Academic Conferences and Publishing International, 2019.

[42] Otzulis, V., and Ozoliņa, Ž. (2017), "Shaping Baltic States defence strategy: Host nation support", Lithuanian Annual Strategic Review, Vol. 15 No. 1, pp. 77-98.

[43] Parrein, P.J. (2011), "De evolutie en toekomst van de Belgisch-Nederlandse marinesamenwerking: Spill-over en politieke samenwerking", Koninklijk Hoger Instituut voor Defensie, Studiecentrum voor Veiligheid en Strategie. Brussel, België.

[44] Plowman, K.D. (2013), "Creating a model to measure relationships: U.S. Army strategic communication", Public Relations Review, Vol. 39 No. 5, pp. 549-557.

[45] Sauer, T. (2015), "Deep cooperation by Belgian defence: Absorbing the impact of declining defence budgets on national capabilities", Defence Studies, Vol. 15 No. 1, pp. 46-62.

[46] Saxi, H.L. (2017), "British and German initiatives for defence cooperation: The Joint Expeditionary Force and the Framework Nations Concept", Defence studies, Vol. 17 No. 2, pp. 171-197.

[47] Susnienė, D., and Purvinis, O. (2015), "Empirical insights on understanding stakeholder influence", Journal of Business Economics and Management, Vol. 16 No.4, pp. 845-860.

[48] Tranfield, D., Denyer, D., and Smart, P. (2003), "Towards a methodology for developing evidence-informed management knowledge by means of systematic review", British Journal of Management, Vol. 14 No. 3, pp. 207-222.

[49] Ušiak, J. (2018), "Security-related cooperation among the V4 States", Politics in Central Europe, Vol. 14 No. 2, pp. 39-56.

[50] Van Dyck, B. (2015), De Belgische veiligheidsstrategie. Onderzoek en aanbevelingen. Koninklijke Militaire School, Brussel, België.

[51] Van Eck, N.J., and Waltman, L. (2013), "VOSviewer manual", Leiden: Univeristeit Leiden, Vol. No.1, pp. 1-53.

[52] Verburg, M. (2020, May 4), "Belgian comprehensive approach", Interviewer: Demeyere, W.

[53] Wallenius, C., Brandow, C., Berglund, A.K., and Jonsson, E. (2019), "Anchoring Sweden's post-conscript military: Insights from elites in the political and military realm, Armed Forces and Society , Vol. 45 No. 3, pp. 452-471.

[54] Wither, J.K. (2020), "Back to the future? Nordic total defence concepts", Defence Studies, Vol. 20 No. 1, pp. 61-81.

[55] Ybarra, C., Bueno, I., Endregard, M., Blatny, J.M., Dugauquier, C., Dhermain, J., Petronio, G., Engman, L.K. (2009), "Counter biological and chemical terrorism", FFI-rapport 2009/00492, Norwegian Defence Research Establishment, Norway.

Appendix 2-1: FINAL PAPER SET

Legend
Scopus
SharePoint
NATO Library
Subject Matter Expert

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
The politics of peace: The challenge of civil-military cooperation in Somalia	George, J.M.	2005	Article	USA	Somalia		
Reliability-seeking networks in complex emergencies	Kruke, B.I.	2005	Article	NA			
De inzet van het Ministerie van defensie bij natuurrampen : Een algemeen overzicht	Leen, G.	2005	Thesis	Belgium			
Agency coordination and the role of the media in disaster management in Hawaii	Prizzia, R.	2005	Article	USA			
Crisis management : A fundamental security task: The NATO experience and Euro-Atlantic partnership	UNK	2006	Magazine	NATO			
Explaining US and British performance in complex expeditionary operations: The civil-military dimension	Egnell, R.	2006	Article	USA	UK		
The EU as a Civil-military crisis manager : Coping with internal security governance	Ehrhart, H.	2006	Article	EU			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
Military force and European strategy	Kaldor, M.	2006	Article	EU			
Coordinating disaster prevention and management in Hawaii	Prizzia, R.	2006	Article	USA			
Shaping the future of UN peace operations: Is there a doctrine in the house?	Ahmed, S.	2007	Article	UN			
Afghanistan: An assessment of conflict and actors in Faryab province to establish a basis for increased Norwegian civilian involvement	Bauck, P.	2007	Report	Norway	Afghanistan		
Security, media and multicultural citizenship: A collaborative ethnography	Gillespie, M.	2007	Article	UK			
Joint civilian/national guard mass casualty exercise provides model for preparedness training	Grant, W.D.	2007	Article	USA			
Rewiring interventions? UK provincial reconstruction teams and 'stabilization'	Jackson, M.	2007	Article	UK			
A clash of mindsets? An insider's account of provincial reconstruction teams	Piiparinen, T.	2007	Article	NA			
Co-ordinating humanitarian operations in peace support missions	Rietjens, S.	2007	Article	Netherlands	Afghanistan		
Sharing information today: Maritime domain awareness	Todd, M.	2007	Magazine	USA			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
Clash of organisational cultures? The challenge of integrating civilian and military efforts in stabilisation operations	Baumann, A.B.	2008	Article	NA			
Towards a new conceptualization of democratization and civil-military relations	Bruneau, T.C.	2008	Article	NA			
A new look at roles and missions	Correll, J.T.	2008	Magazine	USA			
Between reluctance and necessity: The utility of military force in humanitarian and development operations	Egnell, R.	2008	Article	NA			
Emergency management international: Improving national and international disaster preparedness and response	Hecker, E.J.	2008	Article	USA			
Neither fox nor hedgehog: NATO's comprehensive approach and the OSCE's concept of security	Ortiz, A.	2008	Article	NATO	OSCE		
Managing civil-military cooperation: Experiences from the Dutch provincial reconstruction team in Afghanistan	Rietjens, S.	2008	Article	Netherlands	Afghanistan		
National security councils: Their potential functions in democratic civil-military relations	Bruneau, T.C.	2009	Article	NA			
COIN Machine: The British military in Afghanistan	Farrell, T.	2009	Article	UK			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
Humanitarian and military action in armed conflict – Side by side, not hand in hand	Jæger, T.	2009	Article	Norway			
Military crisis management : The challenge of inter-organisationalism	Koops, J.	2009	Other	NA			
British civil-military integration	Korski, D.	2009	Article	UK			
War and medicine	Lillywhite, L.	2009	Article	UK			
Third-generation civil-military relations	Rosén, F.	2009	Working Paper	Denmark			
What kind of homeland security for the European Union?	Sablon, V.	2009	Book chapter	EU			
The doctrinal basis for medical stability operations	Baker, J.B.	2010	Article	USA			
Elements needed to support a crisis management collaboration framework	Beaton, E.K.	2010	Conference Paper	USA			
Collaboration capabilities for crisis management	Beaton, E.K.	2010	Conference Paper	USA			
Involvement of the US Department of Defence in civilian assistance, Part I: A quantitative description of the projects funded by the Overseas Humanitarian, Disaster, and Civic Aid Program	Bourdeaux, M.E.	2010	Article	USA			
The roles of the health sector and health workers before, during and after violent conflict	Buhmann, C.	2010	Article	NA			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
L'approche belge de la réforme du secteur de la sécurité (RSS)	Godts, Q.	2010	Thesis	Belgium			
Integrating civilian and military activities	Lacquement, R.A.	2010	Article	USA			
Managing the civil-military interface in the EU: Creating an organisation fit for purpose	Norheim-Martinsen, P.M.	2010	Article	EU			
NATO's critical infrastructure protection and cyber defence	Smedts, B.	2010	Research paper	NATO			
Bescherming van de nationale kritische infrastructuur tegen een dreiging tot asymmetrische proliferatie	Smedts, B.	2010	Research paper	Belgium			
Esdp and institutional change: The case of Belgium	Vanhoon-acker, S.	2010	Article	EU	Belgium		
Civil protection and disaster medicine in Germany today	Fischer, P.	2011	Article	Germany			
Medical contribution to the comprehensive approach	Fletcher, J.M.	2011	Magazine	UK			
The U.S. Government's medical countermeasure portfolio management for nuclear and radiological emergencies: Synergy from interagency cooperation	Grace, M.B.	2011	Article	USA			
NATO's cyber capabilities: Yesterday, today, and tomorrow	Healey, J.	2011	Other	NATO			
EU crisis management after the Lisbon Treaty: Civil-military coordination and the future of the EU OHQ	Hynek, N.	2011	Article	EU			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
Lessons from EU peace operations	Keohane, D.	2011	Article	EU			
Substantiating the cohesion of the post-cold war US-Japan alliance	Kim, H.-W.	2011	Article	USA	Japan		
The European Commission's Position in the field of security and defence: An unconventional actor at a meeting point	Lavallée, C.	2011	Article	EU			
Disaster preparedness-formalizing a comparative advantage for the department of defence in U.S. global health and foreign policy	Licina, D.	2011	Article	USA			
Civilian crisis management in the EU-structural and functional aspects	Malešič, M.	2011	Article	EU			
How strong is Europeanisation, really? The Danish defence administration and the opt-out from the European security and defence policy	Olsen, G.R.	2011	Article	Denmark			
Engineering for climate change adaptation at the US Army Corps of engineers: Policy, plans, and projects	Dalton, J.C.	2012	Conference Paper	USA			
Risky society, chaotic life: Disaster management laws timely?	Elias, Z.	2012	Conference Paper	Malaysia			
DOD and NGOs in Haiti - A successful partnership	James, T.	2012	Article	USA			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
The comprehensive approach as a strategic design to run the military-industrial complex in operations	Salminen, M.	2012	Conference Paper	NA			
Operationeel rampenmanagement. Case study van de provincie Antwerpen	Van Den Putte, M.	2012	Thesis	Belgium			
Prairie North: A joint civilian/military mass casualty exercise highlights the role of the National Guard in community disaster response.	Vukotich, G.	2012	Article	USA			
Flood risk management: US Army Corps of Engineers and layperson perceptions	Wood, M.	2012	Article	USA			
Global security challenges and critical infrastructure protection in the Republic of Macedonia	Aleksoski, S.	2013	Article	Macedonia			
The European Union building peace near and afar: Monitoring the implementation of international peace agreements	Braniff, M.	2013	Article	EU			
A typology to facilitate multi-agency coordination	Curnin, S.	2013	Conference Paper	NA			
Civil-military coordination for operational effectiveness: Towards a measured approach	Egnell, R.	2013	Article	NA			
'You don't need to love us': Civil-military relations in Afghanistan, 2002 – 2013	Haysom, S.	2013	Article	Afghanistan			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
The future of cyber-resilience in an age of global complexity	Herrington, L.	2013	Article	UK			
From Auftragstaktik to comprehensive approach: Key leader engagement in strategic communication	Hirvelä, A.	2013	Conference Paper	NA			
Fixing U.S. national cybersecurity: A modest proposal for swallowing pride and reducing egos	Iasiello, E.	2013	Article	USA			
The crisis management capability of Japan's self defence forces for un peacekeeping, counter-terrorism, and disaster relief	Ishizuka, K.	2013	Article	Japan			
Creating a model to measure relationships: U.S. Army strategic communication	Plowman, K.D.	2013	Article	USA			
The European Union: A peace actor in the making? Reflections based on the ESDP crisis management operations in Africa	Revelas, K.	2013	Article	EU			
Learning from Afghanistan: Towards a compass for civil-military coordination	Rietjens, S.	2013	Article	Netherlands	Afghanistan		
Introduction: Coordinating actors in complex operations	Ruffa, C.	2013	Article	NA			
The European union as a peace actor	Stivachtis, Y.A.	2013	Article	EU			
Managing transboundary crises: The emergence of European Union capacity	Boin, A.	2014	Article	EU			
Inzet van cybercapaciteiten	Cornille, L.	2014	Thesis	Belgium			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
New security models and public-private partnership (Novi modeli sigurnosti i javno-privatno partnerstvo)	Cvrtila, V.	2014	Article	NA			
Decentralization and decomposability: Determinants of responsive crisis deployment	de Waard, E.	2014	Article	Netherlands			
Normative power under contract? Commercial support to European crisis management operations	Giumelli, F.	2014	Article	EU			
Understanding military decisions and actions in humanitarian assistance operations	Miller, J.	2014	Article	NA			
Serbian civilian capacities for peace operations: Untapped potential	Milošević, M.	2014	Article	Serbia			
The Comprehensive approach – Doctrinal overview and Swedish leadership implications at the operative and tactical level	Ohlsson, A.	2014	Article	Sweden	EU	NATO	
Administrative structures	Sundnes, K.O.	2014	Article	NA			
Young Australians' attitudes to the military and military service	Wadham, B.	2014	Article	Australia			
A comprehensive approach to multidimensional operations	Jasper, S.	2015	Article	NA			
Coastguards in peril: A study of Arctic defence collaboration	Østhagen, A.	2015	Article	Canada	Denmark	Norway	

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
Challenges in coordination: Differences in perception of civil and military organisations by comparing international scientific literature and field experiences	Pramanik, R.	2015	Article	Sweden			
Deep cooperation by Belgian defence: Absorbing the impact of declining defence budgets on national capabilities	Sauer, T.	2015	Article	Belgium			
Comprehensive approach: An appropriate tool to gain security in the new wars and complex emergencies?	Stene, L.K.	2015	Conference Paper	NA			
Comprehensive approaches, diverse coherences: The different levels of policy coherence in the Dutch 3D approach in Afghanistan	van der Lijn, J.	2015	Article	Netherlands	Afghanistan		
De Belgische veiligheidsstrategie. Onderzoek en aanbevelingen	Van Dyck, B.	2015	Thesis	Belgium			
Civil-military cooperation in conflict and post-conflict zones: Needed marriage also for small states? The case study of Slovenian Armed Forces in Kosovo and Afghanistan	Zupančič, R.	2015	Article	Slovenia			
Are we doing enough? Change and continuity in the German approach to crisis management	Allers, R.M.	2016	Article	Germany			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
Capabilities and competencies in humanitarian operations	Apte, A.	2016	Article	USA			
The limits, dilemmas and challenges of European security in uncertain times	Balabán, M.	2016	Article	EU	NATO		
Can Lebanon survive future earthquake disasters by relying on a military response strategy?	Baytiyeh, H.	2016	Article	Lebanon			
"Whole-of-society" peacebuilding: A new approach for forgotten stakeholders	Brunk, D.	2016	Article	NA			
Environmental problems and surge in civil–military cooperation: The case of the Botswana Defence Force	Bugday, A.	2016	Article	Botswana			
Emergency preparedness planning in developed countries: The Swedish case	Kaneberg, E.	2016	Article	Sweden	Poland	Finland	
Britain's emerging cyber-strategy	Lonsdale, D.J.	2016	Article	UK			
Security in the Arctics high politics in the high north	Martin, J.M.R.	2016	Article	Arctic			
België gewapend tegen het terrorisme? Een lezing van het fenomeen en zijn bestrijding: Strategieën en middelen	Scraeyen, L.	2016	Research paper	Belgium			
Designing information systems to facilitate civil-military cooperation in disaster management	Vorraber, W.	2016	Article	Austria			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
The new generation warfare: India's need for comprehensiveness	Ao, T.	2017	Article	India			
Mission assurance: Shifting the focus of cyber defence	Bigelow, B.	2017	Conference Paper	NATO			
Security providers: Obstacles to effectiveness in democracies	Bruneau, T.C.	2017	Article	NA			
'Dialogue, partnership and empowerment for network and information security': The changing role of the private sector from objects of regulation to regulation shapers	Carrapico, H.	2017	Article	NA			
Advanced information systems for enhanced civil-military interoperability in Austria	Gojmerac, I.	2017	Conference Paper	Austria			
La défense contre les menaces hybrides : la Belgique et la stratégie euro-atlantique	Hoorickx, E.	2017	Research Paper	Belgium			
Maritime security and capacity building in the Gulf of Guinea: On comprehensiveness, gaps, and security priorities	Jacobsen, K.L.	2017	Article	Guinea			
Managing military involvement in emergency preparedness in developed countries	Kaneberg, E.	2017	Article	Sweden	Poland	Finland	
Non-medical aspects of civilian–military collaboration in management of major incidents	Khorram-Manesh, A.	2017	Article	Sweden			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
Developing a cyber threat intelligence sharing platform for South African organisations	Mutemwa, M.	2017	Conference Paper	South Africa			
What is the global landpower network and what value might it provide?	Pernin, C.G.	2017	Article	USA			
British and German initiatives for defence cooperation: The Joint Expeditionary Force and the Framework Nations Concept	Saxi, H.L.	2017	Article	Germany	UK		
Healthcare logistics in disaster planning and emergency management: A perspective	VanVactor, J.D.	2017	Article	USA			
Reinvigorating civil–military relationships in building national resilience	Zekulić, V.	2017	Book chapter	NA			
Protecting society in a new era	Endregard, M.	2017	Report	Norway			
Risk in a safe and secure society	UNK	2017	Report	Norway			
Militarization going places?: US forces, aid delivery and memories of military coercion in Uganda and Kenya	Bachmann, J.	2018	Article	USA	Uganda	Kenya	
Patchwork of confusion: The cybersecurity coordination problem	Chaudhary, T.	2018	Article	USA			
Coping with the refugee and migrant crisis in Slovenia: The role of the military	Garb, M.	2018	Article	Slovenia			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
Civil–military relations and organisational preferences regarding the use of the military in Chinese foreign policy: insights from the debate on MOOTW	Ghiselli, A.	2018	Article	China			
Why is there no joint European remotely piloted aircraft system project under the common security and defence policy?	Küsters, C.	2018	Article	EU			
Communications challenges in crisis and transition	Laver, S.	2018	Other	USA			
The crisis of American military assistance: Strategic dithering and Fabergé egg armies	Matisek, J.	2018	Article	USA			
Changes in Norway's societal safety and security measures following the 2011 Oslo terror attacks	Nilsen, M.	2018	Article	Norway	USA		
A conceptual framework for Civil-military interaction in peace support operations	Ooms, D.	2018	Conference Paper	Netherlands			
Advancing cybersecurity from medieval castles to strategic deterrence: A systems approach to cybersecurity	Schannep, J.H.	2018	Conference Paper	USA			
Security-related cooperation among the V4 States	Ušiak, J.	2018	Article	Hungary	Poland	Czech Republic	Slovakia
Support and cooperation	UNK	2018	Report	Norway			
The impact of civilians on defence policy in new democracies: The case of Brazil	Amorim Neto, O.	2019	Article	Brazil			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
What are Military cyberspace operations other than war?	Bigelow, B.	2019	Conference Paper	NATO			
The EU and climate-related security risks: A community of practice in the making?	Bremberg, N.	2019	Article	EU			
Narrative misdirection? UK strategic communication for Afghanistan and beyond	Cawkwell, T.W.	2019	Article	UK			
How can a 'Responsible' European Union contribute to the implementation of the responsibility to protect?	Ercan, P.G.	2019	Article	EU			
Between emergency and routine– securitisation of military security in Iran and Indonesia	Fijałkowski, Ł.	2019	Article	Iran	Indonesia		
The peculiarities of securitising cyberspace: A multi-actor analysis of the construction of cyber threats in the us (2003 – 2016)	Fouad, N.S.	2019	Conference Paper	USA			
An overview of the health services provision in the 2017 Kermanshah Earthquake	Ghanjal, A.	2019	Article	Iran			
Fancy bears and digital trolls: Cyber strategy with a Russian twist	Jensen, B.	2019	Article	Russia			
Managing collaboration in public security networks in the fight against terrorism and organized crime	Kapucu, N.	2019	Article	Turkey			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
Policing the Seas: Building constabulary maritime governance in the Horn of Africa–The case of Djibouti and Kenya	McCabe, R.	2019	Article	Djibouti	Kenya		
Trilateral defence cooperation in the North: An assessment of interoperability between Norway, Sweden and Finland	Møller, J.E.	2019	Article	Norway	Sweden	Finland	
Economic Community of West African States disaster preparedness tabletop exercise: Building regional capacity to enhance health security	Morton Hamer, M.J.	2019	Article	West Africa			
Enhancing global health security: US Africa Command's disaster preparedness program	Morton Hamer, M.J.	2019	Article	Africa			
Social media as the pulse of national security threats: A framework for studying how social media influences young people's safety and security situation picture	Norri-Sederholm, T.	2019	Conference Paper	Finland			
Cooperative bargaining in the EU's common security and defence policy: EUNAVFOR Atalanta	Palm, T.	2019	Article	EU			
Analysis of possibilities for the establishment and implementation of cyber security in the republic of Croatia	Vuksanovic, I.P.	2019	Conference Paper	Croatia			
Anchoring Sweden's post-conscript military: Insights from elites in the political and military realm	Wallenius, C.	2019	Article	Sweden			

Title	1st Author	Year	Type	Country 1	Country 2	Country 3	Country 4
The black sheep of forensic science: Military forensic and technical exploitation	Wilson, L.E.	2019	Article	USA			
Total defence as a comprehensive as a comprehensive approach to national security	Berzina, I.	2019	Book chapter	Latvia			
Back to the future? Nordic total defence concepts	Wither, J.K.	2020	Article	Norway	Finland	Sweden	
Perception of the comprehensive national defence concept in the Latvian and Russian-speaking communities in Latvia	Berzina, I., Zupa, U.	2019	Conference paper	Latvia			

Chapter 3 – THE COMPREHENSIVE APPROACH IN BELGIUM: THE STATE OF AFFAIRS IN 2020 BASED ON A CASE STUDY OF THE BELGIAN DEFENCE

Joaquim Soares*
Royal Military Academy
BELGIUM

Maarten Verburg
Belgian Defence HQ
BELGIUM

Geert Letens
Royal Military Academy
BELGIUM

"In theory, it is always easier to plan, decide and act alone. In practice however, this individualistic vision is an illusion"

– Major General Thys M. as cited by Coelmont and Baddot-Bertrand [5].

DISCLAIMER

The views expressed in this document are the sole responsibility of the authors and do not necessarily reflect the official position of the Royal Military Academy, the Belgian Ministry of Defence, or the Belgian Government.

3.1 INTRODUCTION

Actors across the security spectrum are facing new types of increasingly complex threats (such as hybrid, cyber and terrorism) while having to deal with a persistent lack of resources. As these threats to society easily and rapidly cross the borders between military and civilian organisations, there seems to be no alternative to a coordinated multi-agency approach within a country itself but also amongst international partners and allies [55]. Whilst security actors are increasingly convinced that enhanced cooperation is needed to ensure resilience and safeguard the country and the national interest, international organisations such as NATO and the EU are driving developments in the field [20], [25]. NATO considers resilience as the combination of civil preparedness and military capability as representing a society's ability to resist and recover from shocks through the combination of civilian, economic, commercial, and military factors [51]. Thereby, resilience goes beyond the traditional definition of Civil-Military Cooperation (CIMIC) which focusses on expeditionary operations [58]. During the NATO Warsaw summit in 2016, Member States made a commitment to improve national resilience and recognised "civil preparedness" as the central pillar of this resilience and an important lever for the collective defence of the Alliance. Further, NATO, through the Civil Emergency Planning Committee or CEPC, has drawn up the seven baseline requirements for civil preparedness in support of national resilience. Whereas the CEPC issues recommendations in the seven key baseline areas, reporting on the progress made by Member States is becoming increasingly important as part of the NATO Defence Planning Process or NDPP. With its Global Strategy (2016), the EU also aims to increase resilience in many areas. Through initiatives such as the Permanent Structured Cooperation EU (or PESCO), the EU is now also making resources available to enhance some of the same key areas for civil preparedness and resilience (for example in the military mobility domain). As a Member State and as a Host Nation for the headquarters of both organisations, Belgium must fulfil its commitment to enhancing civil preparedness and resilience. Perhaps surprisingly to some, resilience is also applicable to developed societies where a variety of fragilities may manifest themselves at any given moment in time in domains beyond security, such as economic, environmental, political, and societal [20], [60]. Therefor responses in such cases involve many if not all

* **Corresponding Author**

instruments of power of a state abbreviated as Diplomacy, Information, Military, Economy, Finance, Intelligence, and Law Enforcement (DIMEFIL) [20]. Combatting COVID-19 is a particular test case in this regard that highlights a number of states' fragilities and their resilience level to these as will be duly discussed.

The enhanced level of cooperation amongst security actors, often loosely referred to as the Comprehensive Approach or CA, is supported by a variety of overarching doctrinal concepts and frameworks such as Defence, Diplomacy and Development (3D), Defence, Diplomacy and Development – Law and Order (3D-LO), the Whole of Government approach, the Whole of Society approach, the Integrated Approach, and Total Defence, more or less in this order of magnitude. Common objectives within these different concepts include the pursuit of common situational awareness, common understanding, common 'language', shared objectives, better information exchange, policy coherence and ultimately enhanced efficiency [20]. While antecedents seem to be often threat-, efficiency- and resource-related, consequences range from standardisation, interoperability, a reduction of redundant duplication, the generation of dual use capabilities, enhanced confidence and trust and enhanced effectiveness [5], [73]. The exact doctrinal definition and terminology of the concept is not the focus of this case study however, and the scope is limited to a factual description of the concept as mandated in Belgium. Other existing cooperation mechanisms amongst security actors in Belgium having the potential to reinforce this mandate are also discussed.

In doing so, our study offers several theoretical and practical contributions. First, it contributes to literature by proposing a methodology to further chart elements of CA in nations where the concept may not be fully developed. Our study also offers a conceptual and strategic platform for Belgian Subject Matter Experts (SMEs) to further engage with each other and to further pursue developments in the field. As such, our study challenges the current definition and scope of CA as proposed in national documents and encourages SME's, especially those outside the Ministry of Defence, to revisit their understanding and conceptualisation of CA in light of developments in other NATO and EU countries such as the Total Defence concept and the Integrated Approach as promoted by the EU.

Having introduced the research area and the scope of the study, the remainder of the chapter is structured as follows. First, a background section examines to what extent CA is supported by the national threat perception, national defence objectives and the national interest and values as defined in Belgian defence documents. The research objective and the research questions are subsequently clarified. This is followed by a presentation of the methodology used to generate the answers to the research questions. Thereafter the main findings of the study are presented to include a description of the national command and control structure in the field of CA and a summary of the organisational setup related to civil-military crisis management. A case study of defence aid to the Nation during the COVID-19 crisis then illustrates these findings. Next, a discussion section follows on some of the closely related topics including the roles and responsibilities of the different stakeholders, the standing legal provisions and legal framework, existing joint mechanisms (such as joint planning and training), standardisation (to include standing operating procedures, equipment compatibility, and interoperability), the main challenges to CA implementation in Belgium, and finally Belgian societal perceptions and support. We then conclude with the state of affairs and avenues for further development.

3.2 BACKGROUND

Before discussing CA within Belgium from a Belgian Defence perspective, it is necessary to first look at the threat perception, the national objectives and the priorities of the Belgian Defence as these influences the lens under which CA is approached and understood within the military. The Strategic Vision for Defence [22] promulgated by the Minister of Defence and the subsequent Strategic Environment Review [46] are the foremost strategic guidance documents that characterise the long-term Belgian security environment. While describing the risks and threats facing Belgium as uncertain and complex, several strategic thrusts can be identified including Central Africa and the Great Lakes Region, the Southern periphery of Europe and the Eastern European periphery. CA is cited within several of these strategic thrusts and is defined as follows:

> *The comprehensive approach is an integrated approach to security. It combines the most efficient mix of civil and military policy instruments (not necessarily only hard security actors such as Defence and Police, but also actors working in humanitarian support, development cooperation, justice, education, agriculture ...) to address a security threat in a preventive or reactive manner.*

Several interesting observations can be made from the Strategic Vision document. First, immediately after having been defined, CA is said to be a new term for the earlier 3D or 3D-LO approach [22]. In doing so, the Belgian CA seems to be scoped in a more or less restrictive way despite its original broader definition. Second, a CA (or rather an Integrated Approach) is mostly developed within EU and UNO contexts as these organisations are considered to be most suited for this purpose. The EU sanctions on Russia subsequent to its annexation of Crimea is cited as an example. Strengthening cooperation and coordination between Defence and the other national security actors within a CA (such as Police, Civil Protection, etc.) also seems to fit in the framework of the EU's Security Strategy even if increased NATO interest in the field is also mentioned. Third, the only situation where the Department of Defence is given the lead is in interventions abroad.

In support of the Strategic Vision, the Ministry of Defence sees itself carrying out a number of missions and tasks that are described in various levels of detail in several nested documents including: the Mission Statement [25], the Policy Handbook [26] and the Organisational Plan for Defence 2019 – 2020 [24]. Importantly, in the Mission Statement, there are three key missions and four additional tasks formulated for the Ministry of Defence. The key missions determine the capabilities that the Ministry of Defence must invest in, possess, and train for whereas the four additional tasks are to be executed ad hoc with the available equipment and resources at hand [25].

The key missions are:

- *Contribute to collective defence in defence of the Alliance's territorial integrity;*
- *Contribute to collective security through crisis management operations in multilateral or international contexts, preferably mandated or organised by international security organisations, for the purpose of ensuring global peace and security; and*
- *Protect Belgian nationals worldwide*.

The additional tasks are:

- *Support deployment in the context of internal security;*
- *Execute humanitarian missions that can be carried out both nationally and internationally;*
- *Support defence diplomacy; and*
- *Support the enforcement of international arms control treaties, arms control, non-proliferation and disarmament.* [25]

Whereas CA is not formally mentioned in this document, the need for a National Security Strategy (NSS) to maintain political independence, fulfil national strategic objectives and to protect national interests and values is emphasised with recognised actors being the Federal Public Service Home Affairs (FPS Interior or FPS Int), FPS Foreign Affairs (FPS FA), FPS Economy, FPS Energy, and the Directorate General for Development Cooperation (DGDC). Further, the role of the Armed Forces within the national territory is clearly demarcated. In effect, within the national territory, the Armed Forces may intervene within different scenarios, are only to be used for a limited period, and fall under the responsibility of the authority responsible of the given discipline. Within this context, a discipline is defined as being a functional set of missions carried out by various intervening departments with a total of five disciplines ("rescue operations", "medical, sanitary and psychosocial assistance", "emergency site policing and support to police forces", "logistical support" and "information") being identified in the Royal Decree of 22 May 2019 on emergency planning and emergency management [65].

While the Mission Statement describes what has to be achieved from a Ministry of Defence' perspective, The Policy Handbook further describes how this has to be done. In this document, CA is mentioned twice. First, the emphasis is placed on the possibility that force projection abroad can happen within a comprehensive framework. Second, CA is said to be the privileged method for crisis management with the recognised partners being the other federal departments previously mentioned as well as Regional entities.

It is interesting to note that most if not all the missions and tasks require a CA incorporating either internal or external partners or both. The documents mentioned up to now[2] describing these missions and tasks (or their execution) are internal Ministry of Defence documents however with the focus expectedly being on defence effort and contributions. In the apparent absence of clear higher-order documents and directives formulating interdepartmental and governmental objectives, priorities, and interests (and their realisation), the Ministry of Defence itself has started to look into what could possibly constitute the 'national interest and values'. Defence sees the following themes as its potential constituting elements:

- *Public security in the broad sense to include public order, stability, peace, security, and health;*
- *The integrity of the national territory;*
- *Socio-economic prosperity in a macro-economically and monetarily stable environment;*
- *National sovereignty;*
- *The protection of Belgian values (such as democracy, human right, etc.); and*
- *Having a say in the multinational environment* [25].

These items are generic, similar, but nevertheless a little less vague when compared to the national interest and values as retrievable in the Royal Decree of 18th April 1988 concerning the creation of the to be discussed National Crisis Centre (NCC). Again, looking at the nature of the themes however, it cannot be expected that the Belgian Defence is to realise or safeguard any element by itself. We may therefore conclude that for the preservation of the 'national interest and values' a CA is essential as well. Further, in charting the Belgian CA, we have several expectations. First, we expect to encounter the actors and mechanisms that constitute the traditional pillars of Belgian defence and security policy being NATO, the EU, the UNO and the OSCE [25]. Second, since the 3D and the 3D-LO approach seem to be fairly well established within the defence mind-set, we also expect to often encounter the partners that underlie such an approach. Third, as non-traditional stakeholders (economic, energy, Regional entities, private companies, etc.) are starting to be recognised as actors in the security landscape, we expect to conduct our study in such a way as to also capture these emergent elements that may not yet be fully reflected in internal or even national CA-related documents.

3.3 RESEARCH OBJECTIVE AND RESEARCH QUESTIONS

Given the integration of CA within recent defence strategy documents and the increasing realisation within defence staff that the fulfilment of national objectives requires an inherently comprehensive approach, our main research objective is to chart the current state of CA in Belgium thereby highlighting some of the ongoing discussions and proposing some steps towards increased maturity. As previously stated, our intent is not to dwell upon the exact doctrinal definition and terminology but rather to focus on a more open-ended approach in mapping CA and closely related mechanisms as mandated in Belgium. The underlying research questions are:

- What is the national command and control structure in the field of CA?
- What is the organisational setup related to civil-military crisis management?
- How was defence aid provided to the Nation during the COVID-19 crisis?

[2] One exception, Ref. [37], will be discussed in Section 3.5.1 on the National Command and Control in the Field of CA.

Even if this last research question may not be considered by some to be a 100% CA-related subject in light of the varying definitions and approaches of the concept previously mentioned, it certainly incorporates tangent elements relating to interdepartmental cooperation and relating to defence support to the nation in protecting public health, and thereby can yield some valuable insights.

In answering these three research questions, and through the use of a suitable methodology, our study should provide a guide to further chart elements of CA in nations where the concept may not be fully developed. Besides, it should also offer a conceptual and strategic platform for Belgian Subject Matter Experts (or SMEs) to further engage on the subject with national and international counterparts.

3.4 METHODOLOGY

Belgium is a parliamentary monarchy and a Federal State with governmental organisations operating at different levels: municipal, provincial, community, regional and federal levels. There are 581 Municipalities, ten Provinces, three geographical Regions and three Communities (based on the three official languages being Dutch, French, and German). The total area is 30.500 km^2 for a population of 11.46 million inhabitants. As one may expect, the security landscape is scattered which makes coordination relatively complex. Early in our study, it appeared that there might be a lack of a mature overarching structure regarding CA in Belgium overlooking this complexity and fragmentation. At the same time, preliminary discussions with SME's highlighted the emergent and evolving understanding of CA in Belgium. Therefore, whilst focusing on a description "as is" our strategy also had to account for a puzzle with potentially missing or still not explicit pieces.

3.4.1 Research Design

Our research design combines two main building blocks: first, a conceptual block, and second, an empirical block. In the first block, we exploited the results of a Systematic Literature Review (SLR) to investigate the status quo of CA in the literature thereby providing us with background knowledge for our next building block. Second, we conducted a case study of the Belgian defence using document analysis and interviews where the results of block one served as a skeleton to map the case study findings. The combination of these two building blocks enables us to answer the first two research questions. Additionally, the methodology used can serve as a guide for other nations wanting to assess the depth and breadth of their own CA-related mechanisms. Finally, data collected within the Belgian defence on the ongoing COVID-19 crisis enabled us to provide an illustration of the results pertaining to the first two research questions as mandated by our third research question.

3.4.2 Research Methodology

For block one, we exploited the results of a SLR [66] that investigated comprehensive national defence systems using an overall six-step process proposed by Tranfield et al., [71]. The platforms searched were Scopus, the NATO library and the Belgian national defence database called SharePoint that enabled capturing of a suitable mix of academic and practitioner documents. As part of the results of the SLR, the second review process identified 147 relevant papers after a thorough review of the full paper content.[3] As part of this study, two researchers conducted a review of these 147 papers in order to select the most appropriate papers based on additional selection criteria. These were:

1) Prioritizing later publications;
2) Maintaining diversity in the sample based on the domain or approach (such as cyber, diplomacy, and crisis management);

[3] For more details on the SLR and its process, we refer to the relevant standalone study [66].

3) Ensuring 'geographical' similarity to the studied country by prioritizing publications investigating CA within NATO and EU countries;

4) Ensuring prioritization of journal publications over conference papers; and

5) Excluding publications with a pure supranational focus.

In doing so, we ended up with a body of literature consisting of 40 articles for our background study of block one.

For the case study of the Belgian defence, our focus was first to collect documents directly related to CA in Belgium. In addition, we wanted to collect any document having the potential to form a piece of the developing Belgian CA puzzle. After confirmation from the Belgian military staff on the comprehensiveness of our first block results, (i.e., we had identified all the different aspects and the different types of stakeholders within Belgium as far as CA is concerned), we collected data on each of the main stakeholders' types identified (except intelligence and cyber agencies to permit the publication of this study). Whereas some information and documents were readily available, additional information and documents were obtained through interviews, through requests to the Belgian military staff, through requests to specific Subject Matter Experts (crisis management, strategic communication) and through requests via the academic network of the researchers leading to 63 documents for further data extraction and analysis.

Whereas the level of analysis of the major part of this report pertains to organisations operating at the federal level, which is the level at which most of the defence and security matters are dealt with, suitable references to (organisations operating at) the other levels are made as appropriate. As will be described, the management of an actual crisis or incident in Belgium is based on the nature and the size of the event. Accordingly, the response is managed at the appropriate level: municipal, provincial, or federal [65].

3.5 FINDINGS

3.5.1 National Command and Control in the Field of CA

At this time, two national governmental documents external to the Ministry of Defence imply or promote the use of CA within the defence and security realm. First, the governmental declaration of October 9th, 2014 makes some interesting references to the contributions that the Ministry of Defence is to make in the security and economic domain (security in the streets, safeguarding Belgian economic interests, global maritime and energy flows, information, and cyber environment…). Connecting the often externally focused Ministry of Defence to domestic, social security, and daily issues is one of its merits. Second, the CA Strategy Note of July 20, 2017 [37] describes the Belgian approach to CA in external crisis and builds on past interdepartmental efforts to achieve a more coherent and efficient foreign policy [29]. The Strategy Note was presented by the Ministry of Defence, the DGDC, and the FPS FA and obtained approval from the Federal Council of Ministers. It defines CA as follows (EU definition):

> *To combine, in a coherent and consistent manner, policies and tools ranging from diplomacy, security and defence to finance, trade, development and human rights, as well as justice and migration". […] "The comprehensive approach is both a general working method and a set of concrete measures and processes to improve how the EU, based on a common strategic vision and drawing on its wide array of existing tools and instruments, collectively can develop, embed and deliver more coherent and more effective policies, working practices, actions and results. Its fundamental principles are relevant for the broad spectrum of EU external action.*
>
> Foreign Affairs Council, Council Conclusions on the EU's Comprehensive Approach, Brussels, 12th May 2014.

In spite of this broad Belgian approach to CA, henceforth referred to as the Belgian CA, there is interdepartmental cooperation between the Ministry of Defence, the FPS FA and the DGDC [20], [76]. The DGDC is not a separate Ministry or FPS at this time (the structure and dependencies amongst Belgian federal departments is dependent on Government negotiations), but is a directorate falling under the FPS FA. Nevertheless, it has its own role in this interdepartmental cooperation. In the CA Strategy Note, a triangular cooperation structure is therefore established between the named federal departments and the DGDC with three main underlying structures being the diplomatic missions, the Steering Group (SG), and the Task Forces (TF's) [37]. The diplomatic missions, which report to the FPS FA, are responsible for the exchange of information between any area of interest and Belgium. They also provide a platform for consultations between the various Belgian authorities gathered on site. It is they who have to initiate a CA-related activity and follow-up on its execution [37]. The SG, based in Brussels, meets once a year, and incorporates representatives from the political and administrative levels of various departments including the Prime Minister's Office (PMO), Ministry of Defence, FPS Economy, FPS, Justice, and FPS FA. Whereas there is no specific CA cell or structure within the FPS FA, overall responsibility on CA policy is the responsibility of FPS FA's Policy Planning and Peace Consolidation Department. The director of this department therefore also chairs the CA SG [20]. The SG can in turn set up a Task Force (TF) serving as an interdepartmental consultation platform to analyse a problem or to implement specific decisions taken by the SG [20], [37], [76]. To date, seven TF's have been set up which can be divided into three categories: thematic (three TF's), regional (three TF's) and 'special' (one TF). The three themes covered by the thematic TF's are corruption, raw materials, and risk management. Within the regional TF's, the regions of interest are the Sahel, Tunisia, and Syria [20], [76]. An additional fourth one for Afghanistan is currently under consideration [76]. The 'special' task force deals with civil aspects to crisis management with the aim to contribute to the civilian component of the Common Security and Defence Policy (CSDP) of the EU [76]. Depending on the country, region, or theme for which a TF has been set up, co-chairmanship together with the FPS FA may be attributed [37]. As such, the Ministry of Defence is represented in all TF's relating to security. The TF's generally meet much more regularly than the SG: some quarterly, others even monthly.

In addition to the triangular structure previously discussed, there are also ad hoc structures, predating the promulgation of the CA Strategy Note, which continue to exist. For example:

- 'Table des sables': It is similar to the Sahel TF and meets approximately every month as a working group to discuss the situation in the Sahel Countries [35], [76].
- 'Central Africa Work Group': It is also similar to a TF and meets fortnightly to discuss the situation in Central Africa [35], [76].
- 'PolCiv' meetings: These meetings are organised by the FPS FA in consultation with the other permanent partners being the Ministry of Defence, the Federal Police, the FPS Justice and the DGDC [35]. The meetings take place every fortnight and discussions relate to civil aspects to crisis management [76]. This makes 'PolCiv' the ideal forum to discuss and further develop certain CA aspects [35].
- 'PolMil' meetings: The PolMil meeting are of bigger immediate impact for the Ministry of Defence compared to PolCiv. The meetings take place every Monday and incorporate participants from the PMO, the permanent national representation to the EU, the permanent national representation to NATO, and the administrative and political levels of the FPS FA and the Ministry of Defence. In effect, these meetings are a consultation between the participants on military and security policy, especially on national positions pertaining to ongoing discussions within the EU, NATO, the UN, and the OSCE [76].

While a detailed description of international coordination mechanisms, such as those existing within the structures of the EU, NATO, the UNO, the OSCE, etc. are outside the scope of this study, a few items relating to these mechanisms may be emphasised. First, the FPS FA is responsible for drawing up overall foreign policy [35] and therefore takes on the task of ensuring coordination between the various national

departments before representing the Belgian position within international bodies [20]. Within some of the more important bodies for defence and security, such as the EU and NATO, mechanisms between the Ministry of Defence and the FPS FA can be characterised as permanent so that a common national position is always communicated [35]. Whenever appropriate, in addition to some of the coordinating mechanisms described in the previous paragraphs, an ambassador of the FPS FA will be advised by a dedicated military representative stationed within 'his country' or 'institution'. Second, even if not exactly within the scope of the Belgian CA as such, Belgium has a number of important defence partnerships and Belgian participation can be found in many frameworks more or less associated with CA such as:

- Security Force Agreements (or SFA) and international deployments: Belgium already applies the CA approach within the context of wider supranational endeavours as is the case of EU Training Mission Mali (EUTM), for example.
- B-FAST: The Ministry of Defence is represented within B-FAST (Belgian First Aid and Support Team) which is a Civil Protection instrument at the disposal of the Federal Government to coordinate and sometimes implement the solidarity and crisis mechanisms of the EU, NATO, or the UNO. Its secretariat lies within the FPS FA, but the operational services lie within the Ministry of Defence, FPS Public Health and FPS Int [31], [76]. Notably, it has a separate budget.
- Host Nation Support (HNS): The concept is well known in Belgium as the Host Nation of many NATO and EU institutions. Belgium is also a common contributor in the process of troop reception and onward deployment as in the case of Operation Defender and the enhanced Forward Presence (eFP). Activities such as offloading, coordinating troop movements with partner countries and local entities, checking road and bridge infrastructure, processing and facilitating administrative formalities, obtaining customs clearances, and unloading all require a certain degree of cooperation with civilian authorities [76].
- Military mobility workgroup: This is a standalone workgroup led by the FPS Mobility created on the request of NATO to facilitate some of the administrative and infrastructure related challenges previously mentioned under the HNS framework. With a clear link to the baseline requirements and resilience, it is supported by an EU PESCO initiative [34].
- International Crisis management Cell (ICC): The multidisciplinary ICC was set up by the Council of Ministers on June 28, 2018 as part of the National Crisis Centre (NCC) to ensure the preparation of crisis and risk management at the national level in view of contributing to effective and efficient crisis management on an international level. Thereby the ICC represents Belgium within the EU and NATO for contingency planning and crisis management. Tasks of the ICC include formulating strategic proposals and participation in exercises. Such exercises include the EU's Parallel and Combined Exercise 2018 (PACE18) where the functionalities of the ICC as a critical link between the national and supranational level were tested for the first time, NATO's Crisis Management Exercise or CMX, exercises organised by the Euro-Atlantic Disaster Response Coordination Centre or EADRCC, and exercises organised by the Emergency Response Coordination Centre or ERCC [62].
- Framework Nations Concept (FNC): Belgium participates in some of the clusters within the FNC such as those pertaining to NDPP Goals [4].
- Specific and important partnerships also exist within the realm of major equipment projects with other nations and the industry. The most important and far-reaching military collaborations are with the Netherlands and within the Benelux (Belgium, the Netherlands and Luxembourg) [5], [61], as will be later discussed as part of the BENESAM and Benelux Steering Group initiatives. The breadth and depth of the cooperation between the different countries and partners is heavily dependent on the scope, timing and stage of any given project but is mostly of the MoU and contract type in case of equipment-driven projects and of the intergovernmental strategic partnership type agreement in case of capability-driven programs spanning the full Doctrine, Organisation, Training, Material, Leadership, Personnel, Facilities, and Interoperability (DOTMLPFI) continuum [42].

Examples of such ongoing initiatives and agreements include the CaMo project with France ("Capacité Motorisée" in French or motorised capability), and the F-35 with the USA. Some of these projects may also be supported and realised through cooperation within dedicated structures such as the A400M transport aircraft and the NH90 helicopter. The A400M project is being realised via Organisation Conjointe pour la Coopération en Matière d'Armement (OCCAR) and the NH90 project is being realised via NATO Helicopter Management Agency (NAHEMA).

From the existence of the CA Strategy Note and the structures described above, one may first conclude that the Federal Government and the respective departments are aware of the need for at least a limited CA approach to certain issues. It may be that progress towards implementation of CA within an international context may be influencing the national dynamic. By working closely with organisations who have been advocating some form of CA for some time (such as NATO, the EU, and the UNO), Belgian federal departments may be experiencing top-down pressure towards more integrated cooperation [20]. Second, the intended focus of the Belgian CA lies on countries, regions and themes that are considered relevant because of their immediate impact on Belgian foreign and security policy [35], [37]. In this regard, the Ministry of Defence is driving the concept of Strategic Foresight Analysis based on inputs of a broad variety of partners (including the DGDC, FPS FA, the private sector, and academicians) to analyse the security landscape over an extended period of twenty years. Based on the foresight, five-year plans are intended to drive training, governmental objectives, and security policy. In turn, X+1 and X+2 plans are intended to drive the main effort and more short-term objectives of some of the stakeholders such as the Ministry of Defence and the FPS FA. For the first time, this initiative is being implemented with respect to the Sahel region and can hopefully be extended to other themes and areas in the future. Third, within the current Belgian CA, the nascent 3D-LO approach constitutes an extension to the previously existing 3D vision [20]. The addition of the LO part was necessary given the recent blurring of the boundary between internal and external security in areas such as terrorism and migration [20]. Fourth, the initiative for the further development of interdepartmental cooperation is highly dependent on the Policy Planning and Peace Consolidation Department and on the personal drive of its director [20]. Fifth, the geographically distributed nature of the diplomatic missions enables a local and flexible interpretation to the notion of CA based on the needs within the host country and the importance the mission attaches to CA itself [20], [76]. Finally, but crucially, the CA note is the only official document explicitly focusing on the need for CA within the Belgian defence and security realm to this day. Absent a full-fledged National Security Strategy (NSS) building on this impulse, fragmented top departmental leadership has to vision the national interest and values, has to derive overarching objectives, and has to take on the responsibility to coordinate on a more or less ad hoc basis with partners and stakeholders [76]. The absence of overarching political will in the past is reported as one of the main reasons why steps taken over the past decade to improve interdepartmental cooperation have been limited to the level of mutual consultation and the implementation of some modest ad hoc projects [35].

3.5.2 Organisational Setup Related to Civil-Military Crisis Management

As in other countries, the National (or Federal as is the case in Belgium) Government takes the political decisions concerning the objectives and framework for disaster preparedness and crisis management even if some aspects in Belgium may imply governmental participation at the other levels [65]. The management of an actual crisis is carried out at the level best corresponding to the size and the nature of the event as is illustrated in Figure 3-1. In addition, certain types of crisis response are automatically delegated to the level most deemed appropriate and may be escalated to a higher level in such cases as a lack of necessary means, the crossing of geographical boundaries and a wider than anticipated impact. The three levels are the municipal level for local events (such as floods), the provincial level for larger scale events (such as a Seveso incident) and the federal level for major crisis (such as CBRN and terrorism). At each level, a crisis plan has to be made and regularly updated. At the federal level, the national emergency plan is prepared in consultation with all the departments and actors involved in a crisis and contains the following elements: Risk analysis, global organisation of the departments and emergency help, and preparations for inter-

departmental crisis management [81]. Besides the 2019 law previously mentioned, the other important documents in this domain include the Civil Security Law of 15 May 2007 and Royal Decree of 10 June 2014 regarding the roles and responsibilities of some of the first responders.

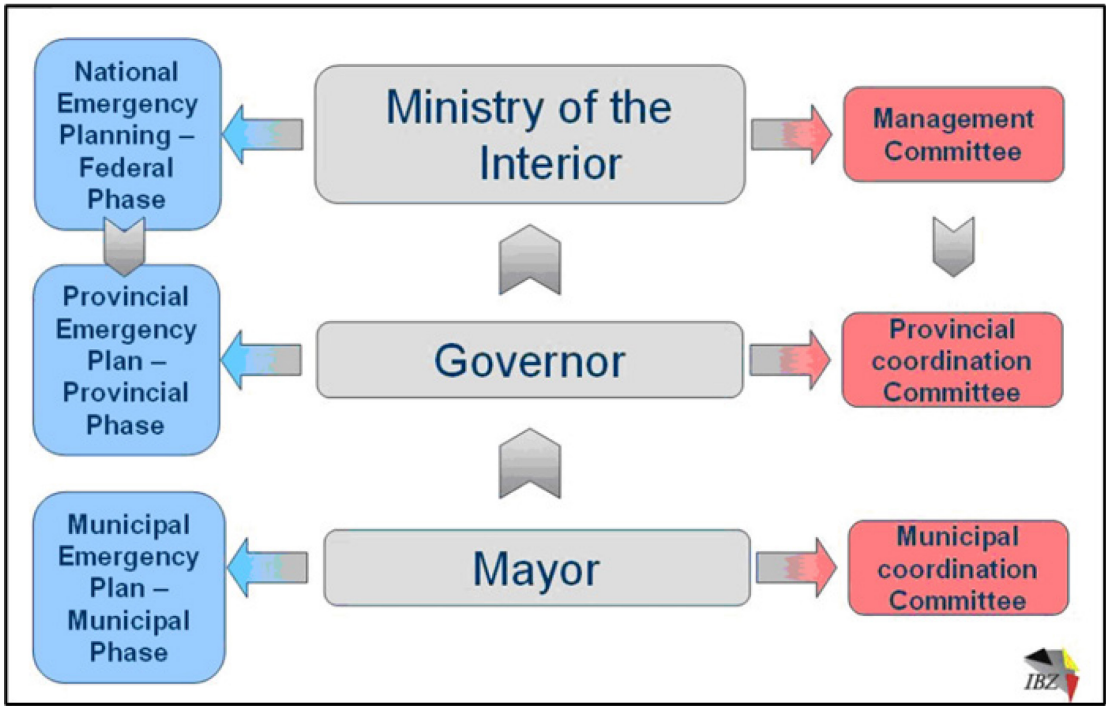

Figure 3-1: Emergency Preparedness and Response in Belgium (FPS Int [38] as cited by Ybarra et al., [81]).

At the federal level, there are a number of bodies responsible for coordination between departments and governmental authorities at other levels. First, the National Security Council (NSC) was established by the Federal Government in 2015 (Royal Decree of January 28, 2015) as a step towards better coordination of security policy [20], [72]. The NSC consists of the Prime Minister, all Deputy Prime Ministers, the Minister of the Interior, the Minister of Foreign Affairs, the Minister of Defence, and the Minister of Justice [76]. In addition, a number of SME's may be invited depending on the situation. Examples of previous invitees include the Director of the National Crisis Centre, the Commissioner General of the Federal Police, the Federal Public Prosecutor, and health experts [29]. Two bodies work directly under the NSC: The Coordination Committee for Information and Security (CCIV) and the Strategic Committee for Information and Security (SCIV). The CCIV is made up of staff from different administrations including the Federal Police, the National Crisis Centre, FPS FA, the and the different intelligence services [29]. The Chief of Defence is also invited in an informal capacity since Nov 2018 pending a revision of the Royal Decree to permit his formal inclusion. This committee is tasked with various security matters and consists of focused working groups [72], [76]. Examples of some of the working groups include those dealing with terror, disinformation, the protection of scientific potential, and hybrid threats [76]. There is also a working group being constituted to delve into the development of a national security strategy following the new Federal Government pact 2020 – 2024 [14], [76]. The SCIV in turn forms the link between the CCIV and the NSC. Whereas the SCIV consists of the same actors as in the CCIV, the analyses and decisions are made from a higher political level perspective [76]. From a military point of view, the CCIV, the SCIV and the NSC can be compared to the tactical, the operational, and the strategic levels, respectively [76].

Second, the National Coordination and Crisis Centre (NCC) was formally set up by the Royal Decree of 11th Apr 1988 as part of the FPS Int to constitute the federal or strategic level of crisis preparedness and response. The tasks of the NCC include:

- *Organisation and coordination of emergency planning and cooperation with the authorities involved;*
- *Drawing up of cooperation procedures with other departments and/or provincial, national and international institutions;*
- *Cooperation between the 5 disciplines of help and emergency services;*[4]
- *Development of crisis management know-how;*
- *Ensure the following:*
  - *Well-founded decision making based on the assessment of the situation;*
  - *Coordination of the means to be used;*
  - *Information to the public; and*
  - *Contacts with foreign Countries as well as with European and International Organisations".* [81].

The NCC is therefore responsible for the full spectrum of the crisis risk management cycle including analysis, preparation, planning, and management and is accordingly composed, amongst other units, of a directorate Critical Infrastructure Protection and Risk Assessment (CIPRA), a directorate emergency planning, and a directorate incident and crisis management beside the previously mentioned ICC [62]. As part of its risk assessment role, the directorate risk assessment prepares an interdepartmental and interdisciplinary (including NGOs, academicians, and private partners) risk inventory document called the Belgian National Risk Assessment (BNRA) extrapolating from past incidents and crisis' and modern trends. This inventory is then passed on to the directorate emergency planning for development and operationalisation of emergency plans and preparations. If the risk materialises, it is then handled by the directorate incident and crisis management based on the appropriate plan. Through underlying interdepartmental workgroups, the NCC is also tasked with the follow-up and development of the seven baseline requirements. As such, the Director General of the NCC serves as the Belgian representative to the CEPC. In this regard, the role of the ICC can be reemphasised as it functions as the nodal point for civil-military cooperation pertaining to the EU and NATO. Besides participating on behalf of the NCC in emergency planning exercises, the ICC coordinates any requests arising from the EU and NATO crisis management authorities towards the national stakeholders as in the case of recent COVID-related requests for example. Another noteworthy interdepartmental collaboration taking place within the purview of the NCC is the multidisciplinary Chemical Biological Radiological and Nuclear explosives (CBRNe) platform and centre of expertise based on a MoU signed between the FPS interior, the Minister of Defence, and the FPS Public Health. The CBRNe centre of expertise brings together experts from different CBRN-related bodies (including the FPS Public Health, the Ministry of Defence, the Federal Police, the FPS Int, Federal Agency for Nuclear Control (FANC) and Sciensano[5] to work together and with the coordinators of the NCC with a view to:

- Prepare for CBRNe emergencies;
- Perform crisis management and response during real CBRNe emergencies; and

[4] The five disciplines are "rescue operations", "medical, sanitary and psychosocial assistance", "emergency site policing and support to police forces", "logistical support" and "information" as identified in the Royal Decree of 22 May 2019 on emergency planning and emergency management [65].

[5] Sciensano is the federal scientific institution of public health operating under the authority of the Federal Minister of Public Health and the Federal Minister of Agriculture.

- Ensure integration and coordination between the aspects of "public order and security" on the one hand and "public safety" on the other hand during CBRNe-type emergencies [57].

Third, the autonomous Coordination Unit for Threat Analysis (CUTA), which is under the joint authority of the FPS Int and FPS Justice, is responsible for making and coordinating threat analyses for the benefit of the different Governments [72]. Intelligence services such as the military General Intelligence and Security Service (ADIV) and the civilian State Security Service (VSSE) play an important role within OCAD and in many of the previously mentioned working groups of the CCIV. Both intelligence services also share an information warfare platform that has been particularly active lately as will also be discussed in the section relating to the COVID-19 pandemic. The platform was created in 2019 to help combat the spread of disinformation and external manipulation in the context of national and European elections [68]. Its main tasks are the monitoring, the detection and the analysis of information disseminated via the media, especially via social media and networks [68]. It reports within Defence to national and international stakeholders [68].

Fourth, the cyber domain is also one benefitting from the creation of a coordinating body: The Centre for Cyber Security Belgium (CCB). The mission of the CCB is to coordinate between the various cyber instances in Belgium (which are spread across different departments including the Ministry of Defence and the Federal Police amongst others), to raise national awareness on cyber threats, to provide specialist training and education, and to draw a national division of tasks so that the contributing bodies can focus on their respective core business [7]. The exact role and contributions of the OCAD, the CCB and the intelligence services will not be further discussed due to the technical nature of their work and due to the classification and publicity requirements of this study.

Regular exercises take place at the different levels between the aforementioned bodies and responders such as the Police, Fire Brigade, Ambulance Service (SAMU), and Civil Protection [81]. Where available and needed, military units are mostly involved on an ad hoc basis [29]. As such, most collaborations with the military take place at the provincial level where the Governor is assisted by a dedicated military commander (generally OF-5) and staff [18]. In real crises however, the Federal Government can decide to deploy military capabilities within national territory [22]. Examples include the ongoing deployment in support of internal security under the banner Operation Vigilant Guardian (OVG) consequent to the 2015 Paris terrorist attacks and, more recently, the deployment of specific capabilities in support of public health to fight the COVID-19 pandemic. Deployment of the military in support of internal security objectives is quite sensitive however with the Police retaining overall responsibility [72]. In effect, the Ministry of Defence is intended to play a temporary and mostly supporting role during internal deployments. Many exceptions exist based on MoUs between the Ministry of Defence and the different FPS' mainly pertaining to either symbolism (MoU pertaining to the protection of the Federal Parliament, MoU pertaining to the protection of the Prime Minister's residence, etc.), pertaining to domains where specific competencies are not available within the civilian realm (MoU pertaining to Explosive Ordnance Disposal (SEDEE/DOVO), MoU pertaining to air policing (QRA), MoU pertaining to the Aviation Safety Directorate (ASD), MoU pertaining to the use of Unmanned Aerial Systems (UAS) for maritime pollution detection…) and to situations where collaboration with the Ministry of Defence is essential (different MoU's with the Federal Police, MoU pertaining to the National Airspace Security Centre (NASC), MoU pertaining to the Maritime Information Centre (MIK), MoU pertaining to the Maritime Incident Response Group (MIRG), MoU on the transport of vital organs for transplants…). In such exceptions, military presence and support can be characterised as permanent.

Whereas the crisis management architecture is Belgium-centric (with usual actors identified being Fire Fighters, Civil Protection, Police Force…), the 'Belgian CA' currently resembles the 3D-LO concept but is ultimately intended to be in harmony with Belgium's foreign policy, which itself is aligned with the agreements and alliances existing at the supranational or multilateral level (especially the EU Global Strategy and its underlying Integrated Approach). It can therefore be summarised that CA in Belgium mainly has two components: the often internally- and safety-focused crisis management architecture and the often

externally-and security-focused 'Belgian CA'. Belgian SME's and doctrinal documents seem to focus on one of the aspects only whereas recent crisis on the national territory (terrorism, COVID…) seem to indicate that military tools are required to reinforce public safety and that there is a clear security-related aspect to these challenges. At the same times external crisis (Sahel, Afghanistan, Iraq…) also testify that the military needs to be supported by such partners such as FPS Int, FPS Justice, Federal Police… In doing so, there seems to be no boundary but rather a clear continuum between these the internal and external aspects. Further developing this nexus and inducing cooperation across what sometimes still seems like a hard boundary is an interesting avenue for the further development of CA in Belgium.

3.5.3 Defence Aid to the Nation During the COVID-19 Crisis

In the face of the COVID-19 pandemic and with the activation of the federal phase in crisis response, the NSC was reinforced through the participation of regional and community leaders. More precisely, the Comité Fédéral de Coordination or COFECO supported by the NCC took on added responsibility. It established a Federal Coronavirus Task Force under the leadership of Federal Minister Philippe De Backer to bring additional medical supplies and devices such as mouth masks into the country [8], [75]. Initially the Task Force consisted of four different working groups, each dealing with its own focal point, but a fourth under the leadership of the Ministry of Defence was created to focus on logistics and distribution [8]. The role of provincial coordination mechanisms within which the Ministry of Defence actively participates was equally important [39]. At this level, military commanders and their staff advising the Governor facilitated and coordinated requests for support arising from the respective provinces, checking them against the support that the Ministry of Defence could effectively provide [70].

Within this context, many steps were taken by the Ministry of Defence to support the Task Force and the nation during the COVID-19 pandemic. Most of the support provided was of medical nature and provided directly or indirectly at the request of the FPS Public Health. For this purpose, medical planners (officers from Medical HQ) were embedded within the FPS Public Health in a Liaison Officer (LO) role [15], [19]; [27]. Together with the three FPS health inspectors (one per Region), they determined the needs in- and priorities for defence support which were then sent to a specially created coordination cell at the Medical HQ [15], [19]. This cell was then responsible for the practical organisation of all the support provided by medical units [15], [19]. For simplicity, only a summary of the help effectively provided is discussed even if other capabilities, personnel, and equipment were, or continue to be, placed on standby [6]. First, the Ministry of Defence was tasked with the purchasing and the distribution of 18 million mouth masks amongst other medical equipment [8], [27], [75]. For this purpose, the military barracks in Peutie (in the centre of the country, near Brussels and near Brussels Airport) serves as the main logistical hub for the reception and the onward distribution towards eleven provincial military and civilian hubs [8], [27], [74], [75]. From these provincial hubs, equipment is further tested and distributed to users such as hospitals and retirement homes in collaboration with Civil Protection [78]. Distributed equipment mostly includes internally and externally purchased masks but also disinfection gel, glasses, overalls, and gloves amongst other Personal Protective Equipment (or PPE) [27]. The FPS Public Health is responsible for determining the distribution key (who gets what and how much) whereas the Ministry of Defence is 'only' tasked with the execution [8]. The benefit of at least one military base able to serve as a hub in each province is one of the lessons learnt by the Ministry of Defence from the pandemic [74]. Second, military ambulances and personnel were deployed to transport coronavirus patients to appropriate hospitals [15], [27]. The main aim was to ensure patient regulation and distribution given the high occupancy rates of Intensive Care (IC) beds in certain Belgian provinces. Third, medical personnel were deployed in a supporting logistical role in retirement homes all over the country [13], [27]. Tasks included disinfection of rooms where residents had died and help in serving meals [13], [27]. Fourth, fifteen places were made available in the military hospital morgue [27]. Fifth, the military hospital admitted all victims of acute burns (which is one of its core-competencies) from all around the country to free resources in civilian hospitals [27]. Six, equipment including ventilators was provided to different hospitals [27]. Seven, wherever required, disinfection teams were deployed including for disinfection of aircraft,

ambulances, and the previously mentioned rooms in retirement homes [27]. Eight, testing teams were deployed to directly test patients and testing equipment was loaned to civilian laboratories [9], [27], [16] Nine, the defence lab (DLD) was requested to perform quality tests on masks [27]. Ten, medical personnel were sent as re-enforcements to work directly within certain hospitals [27]. Eleven, equipment was provided for the establishment of triage centres [27]. Twelve, decontamination equipment was provided to a fire brigade unit [70]. Thirteen, equipment and supplies were distributed to the homeless in big cities and to centres for psychologically impaired and handicapped people [6]; [27].

In addition to this support of medical nature, non-medical support was provided to the FPS FA. First, Belgian, and European nationals abroad were repatriated via the military airport of Melsbroek. Second, the airport fuel pumping station provided supplies to the civilian airport of Liège which is playing an important role as a European hub for medical supplies [27], [53]. Third, aid was delivered overseas via the military airport [27]. Finally yet importantly, the military intelligence service (or ADIV) and the civilian State Security Service (VSSE) have had their part to play in the context of the previously mentioned information warfare platform combatting fake news and actors attempting to exploit the pandemic conditions [27], [68]. Propaganda via social media seems to be very effective in times of COVID-19 as people who are unsure or afraid of what is happening actively seek out more information [68]. For example, the many images and videos of certain countries' planes delivering equipment to help European Nations in stopping the spread of COVID-19 may be precisely intended to tag an image of failure on EU and NATO members and institutions [68]. The task is substantial given the colossal influx of information, but specialists are able to detect clues and identify influencers [68].

Figure 3-2 provides an overview of Defence resources deployed during the peak of the pandemic.

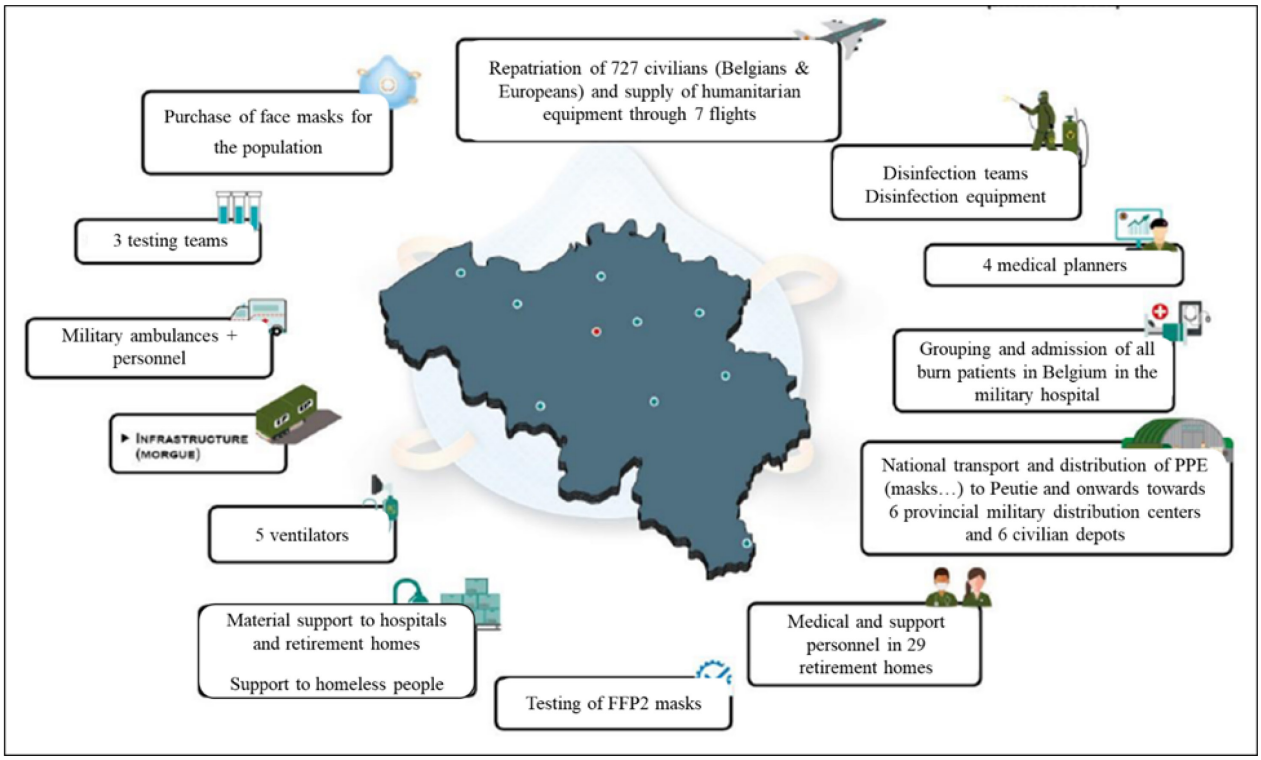

Figure 3-2: Defence Resources Deployed During the Pandemic [27].

Ongoing missions also continued to be carried out with minimal disruption including the Baltic Air Policing (BAP), enhanced Forward Presence (eFP), Operation Vigilant Guardian (OVG), Quick Reaction Alert (QRA), European Union Training Mission (EUTM – Mali), Operation Resolute Support (ORS, Afghanistan), Explosive Ordnance Disposal (EOD) on national territory, Search and Rescue at sea (SAR) as well as the planned deployment of naval ships [1], [6], [27], [69], [77]. For this purpose, a variety of preventive and risk mitigation steps are taken such as pre-deployment screening, pre-deployment isolation, on-board quarantine in case of Navy ships, reduced level of contact with people external to the mission, scrapping of stopovers in case of Navy ships, and post-deployment screening [6], [69], [78]. Figure 3-3 provides a general overview of the regions where the Ministry of Defence is actively following local COVID-19 related conditions either due to ongoing operations or due to the posting of Belgian military personnel.

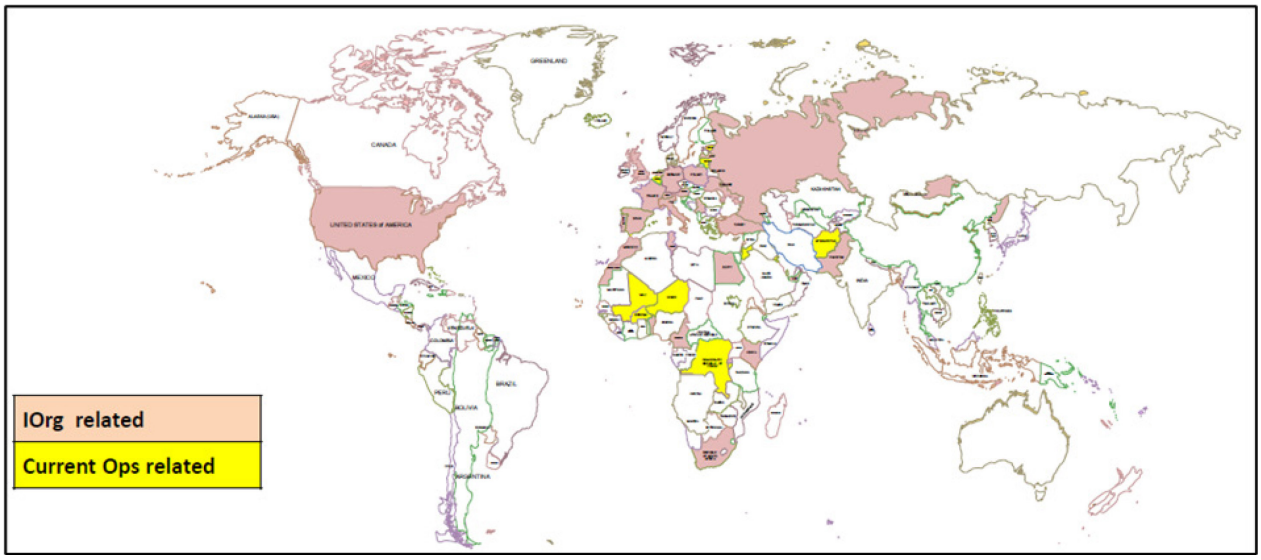

Figure 3-3: Follow-Up COVID-19 on BEL Areas of Interest [28].

3.6 DISCUSSION

3.6.1 Roles and Responsibilities of the Different Stakeholders

The most important stakeholders within the 'Belgian CA' and in the domain of crisis management have already been mentioned in the previous sections within the context of the structures in which they operate. In this sub-section, our intent is to delve more into detail into the roles, responsibilities, expectations, attitudes towards CA and attitudes towards the Ministry of Defence that characterises some of these defence-stakeholder relationships. In doing so, the order in which the stakeholders are listed corresponds more or less to the order in which they appeared in the previous sections.

The FPS Foreign Affairs: The FPS FA strives for more interdepartmental cooperation because of the need for a more coherent foreign policy and because of top-down pressure stemming from an increasingly Integrated Approach followed within International Organisations [20]. Given its responsibility in the foreign policy domain and the narrow vision of the 'Belgian CA', the FPS FA takes the lead in organising interdepartmental cooperation [35]. The other departments also expect the FPS FA to lead most CA-related initiatives. Even if the exact expectations of the FPS Foreign Affairs from the other departments may not be clear (yet), it can generally be said that the FPS FA expects partners to make a good contribution to the implementation of foreign policy.

The Directorate General Development Cooperation: According to the governmental coalition agreement, the main objective of the DGDC is the Sustainable Development Goals (SDG) in general and the fight against poverty in particular [29]. However, when linked to climate change, migration and the fight against terrorism, the security links and implications cannot be ignored [35]. The DGDC is also open to more interdepartmental cooperation and to CA as can be testified by the recently signed MoU between its privileged autonomous partner ENABEL[6] and the Ministry of Defence and the DGDC's own strategy note titled Policy Framework for Belgian Development Cooperation in the Security Sector [32]. Governance for Development (G4D), which is a think thank linked to the DGDC, is also currently advocating for a more integrated approach to fulfil policy objectives as can be seen in their proposed framework (Figure 3-4).

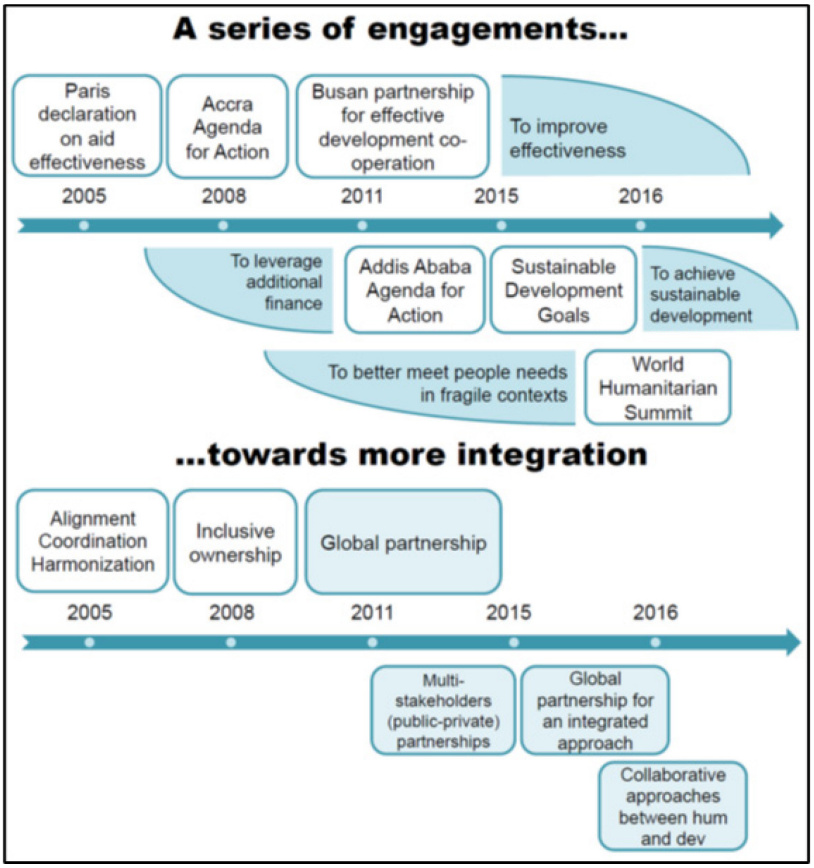

Figure 3-4: G4D Framework Towards More Integration [40], [41].

The Ministry of Defence: The Government wants to retain an effective foreign and development aid policy next to a broadly deployable military because it is the most efficient way to deal with current security challenges [22]. As a result, it can be said that the Government primarily expects the Ministry of Defence to carry out its tasks in an effective manner despite the limited means at its disposal. On the other hand, the Ministry of Defence expects the Government to draw up a coherent defence policy in line with a National Security Strategy and to support both doctrines with adequate means. All indications are that the Ministry of Defence supports the further expansion of the 'Belgian CA' and interdepartmental cooperation within the context of crisis management. For example, the defence policy handbook [26] states that the comprehensive approach is the recommended way to handle fragile contexts (e.g., Sahel, MENA, Middle East, Caucasus, Belarus…) and to respond to modern crises (including hybrid threats, Russia, IS, cyber threats, revival of Great Power Competition, etc.).

[6] ENABEL is the development agency of Belgium's Federal Government.

International Organisations: While a detailed discussion on the roles, responsibilities and relationships between the Ministry of Defence and the numerous International Organisations within which Belgium has an active security-related participation is not within the scope of this study, and many key aspects pertaining to key International Organisations have been discussed in the previous sections, a few relevant topics may still be emphasised. First, NATO is primarily concerned with collective defence. By focusing on resilience and civil preparedness via the CEPC and its seven baseline requirements, NATO intends to enhance civil preparedness as part of the NATO Defence Planning Process (NDPP). Since NATO is one of the pillars of Belgium's security policy, Belgium is expected to maintain this transatlantic link in the future, including within the context of any future CA- and Belgian National Security Strategy-related developments [72]. Second, even if the Ministry of Defence strives to fulfil its contribution to NATO forces and operations [26], there is a lot of criticism within NATO towards those countries (including Belgium) that do not spend 2% of their GDP on defence [63]. So, maintaining and building upon the existing transatlantic relationship in times of resource scarcity is an active challenge. Third and importantly, the EU currently aspires to do more in the security domain as a means to broaden and deepen EU integration [50]. Belgian diplomacy and the Belgian Defence fully subscribe to the EU's Global Strategy (2016) and objectives. In effect, the EU's approach to crises and security is inherently integrated i.e., multi-dimensional (diplomacy, security, defence, finance, trade, development and humanitarian aid), multi-level (local, national, regional and global levels), multi-phase (prevention, crisis management, stabilisation and peacebuilding) and multilateral (Member States, EU institutions, international partners, regional partners, civil society organisations) [20]. Working within this EU framework gives Belgian foreign and defence policy a more substantive direction and new supporting mechanisms such as PESCO and the EDF may offer opportunities to counter resource scarcity at the national level [63].

France, Luxembourg, and The Netherlands as privileged partners: While the collaboration between the different countries within the Benelux and CaMo frameworks will be discussed in the 'Joint Planning, Training, and Procurement section', the partners have similar expectations. For example, within the context of the Belgian-Dutch naval cooperation, both countries hope to maintain their military capabilities, maintain their operational readiness, maximise synergies, optimize supply-chains and increase their interoperability [29], [61]. The most important driver for both countries is to achieve these objectives in a cost-and personnel-efficient manner [5], [29], [30], [61]. These motivations also drive the CaMo project even if the project is also a means to supporting bottom-up European defence [23].

Coordinating bodies: In times of crisis, the actions of the different actors will be coordinated (for example by the NCC) under the principle that the service or entity that is responsible under normal conditions also retains overall responsibility during the crisis condition [81]. The expectations and roles of the different actors will vary according to the circumstances. However, the general expectation amongst partners is that the bodies will coordinate efforts and divide tasks appropriately. This should go some way in countering resource limitations and enable participants to focus on their respective core-business in critical times [7]. The coordinating bodies and other partners within them will in turn expect the Ministry of Defence to carry out the job assigned to it properly, with good information sharing and transparency [29].

Humanitarian and Non-Governmental Organisations (NGOs): NGOs can fulfil a variety of tasks in diverse domains. For example, in the case of the COVID-19 epidemic, the Red Cross alone was involved in blood product supplies, the installation of triage posts, providing logistic support such as ambulances for transport of patients, the distribution of basic supplies such as food and water, and the provision of psychosocial assistance to patients and family members of victims. While tasks and areas of interest often overlap, according to Luyckx, NGOs only expect support from the military when it is strictly needed [54]. As cooperation with military organisations may imperil the perception on principles such as neutrality, impartiality, humanity and independence, many NGO's may want to have as small a relationship with the Ministry of Defence as possible [32], [54]. Still according to Luyckx, the literature mentions that defence organisation sometimes cooperates with humanitarian organisations for image-polishing purposes only [54]. More attention may therefore be needed on creating and sustaining relationships with these type of stakeholders as compared to others.

First responders: It is not possible to perform a complete analysis of the responsibilities and expectations of each responder with respect to the Ministry of Defence and inversely within this study. However, one can summarise that first responders fulfil a variety of critical tasks during a crisis as is illustrated by the 'golden hour' evacuation principle widely disseminated within the military. For example, the Police performs tasks including securing the area, avoiding disruptive entry, and facilitating the movement of other first responders and the evacuation of people [81]. Fire Brigade responsibilities includes mitigation in the event of fires, floods, mass casualties, and chemical leakages. During such events, they are also responsible for the rescue and the initial evacuation of injured people within the context of discipline one [81]. Civil Protection personnel are in turn called upon when specialised material is needed or when the fire brigade has insufficient resources at hand. There are synergies between many of these stakeholders and the military which is usually formalized in a MoU at the departmental level. Many examples of such MoU's have been provided in the "Organisational setup related to civil-military crisis management" section including the MoU pertaining to Explosive Ordnance Disposal (EOD), the MoU with the Federal Police, and the MoU with firefighting services on firefighting wildfires. In some cases, collaboration can also be formalized up to the local level based on SOPs between specialised defence units and local stakeholders. For example, there are SOPs between the military ambulance service and the civilian ambulance service operating in the Brussels Region.

Hospitals: Hospitals receive patients, treat them and are responsible for the follow-up of patients to include tracing [81]. In case hospitals are overrun by the number of patients, they have to redirect the patients through ambulances to other pre-recognised medical facilities, as was the case during the COVID-19 pandemic. Military and the Red Cross ambulances were pressed into action as civilian ambulances were overrun by demand [15], [27]. Importantly the only military hospital in Neder-Over-Hembeek (near Brussels) also has a certain crisis intake responsibility (disaster hospital), and medical units have capabilities pertaining to the deployment of fields hospitals. A detailed description of the role played by the medical military units and the military hospital is provided in the section pertaining to the COVID-19 pandemic.

Society and the Population: The society and the population of Belgium mainly have expectations with respect to the Ministry of Defence in the context of aid to the nation where the military must intervene in case of insufficiency of civilian resources [10]. Dumoulin points out that this task of aiding the nation is important as it permits interactions between the civilian and military world [33]. On the other hand, the Ministry of Defence and its personnel expects support from the population in order to be able to carry out its missions and tasks [5], [33]. In particular, there is a need to have a general appreciation of the work being done. This leads to a good image and a positive impact on recruitment and budgetary resources [5]. For this purpose, there is an ongoing focus on a well-developed strategic communication strategy and plan [29] which will be discussed in the section 'Societal Perceptions and Support'.

The Media: Agenda-setting or the emphasis on certain issues by the media such as conflicts impact the perception of performance of national leaders by the population. Such media impact or priming of political judgements is regulated by citizens' level of political knowledge, exposure to political views, and interest in conflict [47], [49]. Media framing of the coverage content is also an important parameter in determining public support for issues including crisis response options (such as diplomatic, military, etc.) or for the level of military spending [44], [47]. According to Sigelman et al., there is also an erosive effect of the accumulation of events in cases where a foreign policy crisis drags on unresolved [67]. In a similar fashion, the media is also able to influence other stakeholders such as politicians and parliament [12]. Additionally, the media has the increasingly important and difficult role of fact-checking information, which is becoming increasingly important in the age of "fake news". The public then needs to be informed in such a constructive way as to avoid rumours and the spread of confusion [29], [81]. When media knowledge of military matters is deficient and the will to fact check information absent, an opportunity is presented for vested interests to control the news cycle [48].

Outsourcing Partners: Although not a part of the 'Belgian CA' or the Belgian crisis management architecture as such, this section is incorporated for completeness given current developments and future opportunities in the field. As in many other countries, many outsourcing partnerships and contracts can be identified within the Ministry of Defence. In Belgium, this aspect is currently limited to non-core-business and mostly non-security tasks such as leasing, IT, catering, cleaning, and maintenance. Expectations of the Ministry of Defence include budget savings, the freeing of internal resources to the benefit of core-business continuity, achievement of better service levels, and higher levels of personnel satisfaction [3]. It can be assumed that outsourcing partners, like other companies in the private sector, expect to benefit financially and sustainably from this collaboration. The main drivers for such cooperation are the limited amount of personnel and budgets available to carry out the main organisational business on the one hand and the financial rewards on the other hand. Given the drivers and limitations, the cooperation in this field is generally structured around a contract and contractual law.

3.6.2 Standing Legal Provisions and Legal Framework

The legal framework on which the cooperation between the Ministry of Defence and a stakeholder is based can vary considerably from one stakeholder to another. There are many options, and a single relationship may also exist on the basis of several different types of documents at the same time. First, various international Treaties (such as the Lisbon Treaty with its article 42.7 on collective defence and the Washington Treaty with its A5 on collective defence) can be placed at the very top of the legal hierarchy at least as far as the 'Belgian CA' is concerned. Such Treaties may be supplemented by Agreements and Protocols. For example, NATO's Partnership Interoperability Initiative (PII) aims to improve operational effectiveness in NATO-led operations and the Enhanced Opportunities Partnership (EOP) program offers opportunities to some countries to work more closely with the Alliance [56]. Another example are the various Host Nation Support agreements signed within NATO [56]. Interestingly, some Agreements and Treaties are only valid in peacetime and others unintentionally or deliberately leave a grey zone in case of war [29]. Treaties and Agreements are often ratified and transposed in national laws, which are also the most important legal frame of reference for the national crisis management architecture. Amongst the most important for Belgium, the Law of 20 May 1994 'concerning the use of the Armed Forces' determines the deployments of the Armed Forces outside wartime and the authority to make decisions on the deployment of the Armed Forces [72]. Specific laws may also exist for particular domains such as the Intelligence Services Act of 1998 laying down the tasks of the Intelligence Services [7], [64]. In Belgium, Royal and Ministerial Decrees usually complete, interpret or implement national laws, for example the Royal Decree of 6 July 1994 implementing the Act of 20 May 1994 cited above [72], the Royal Decree of 22 May 2019 relating to emergency planning [18], [81], and the Royal Decree of 28 Jan 2015 establishing the National Security Council. Perhaps the most important documents, along with the respective Laws and Royal Decrees, are the numerous MoU's existing between stakeholders and the Ministry of Defence including the MoU pertaining to Explosive Ordnance Disposal (EOD), the MoU pertaining to air policing (QRA), the MoU pertaining to the Aviation Safety Directorate (ASD), the MoU pertaining to the use of Unmanned Aerial Systems (UAS) for maritime pollution detection, the MoU with the Federal Police pertaining to the anti-terror operation OVG, the MoU pertaining to the National Airspace Security Centre (NASC), the MoU pertaining to the Maritime Information Centre (MIK), and the MoU pertaining to the Maritime Incident Response Group (MIRG). Other forms of documents identified within the course of this study include STANAGS (or standardisation agreements such as the AJP-9 in case of the NATO understanding of civil-military cooperation), SOPs (as previously mentioned within cooperation amongst ambulance services), governmental strategy notes (such as the CA Strategy Note of 2017), national plans (such as national emergency response plans drawn within the purview of the NCC), department strategy notes (Such as the Mission Statement for Defence of 2019), Letters of Intent (LOIs as sent to industrial partners for example), and contracts (as in the case of outsourcing and procurement). Ultimately, the existing trust-level between the partners, the degree of assurance desired, the intended grey area, the intended durability of the relationship and the amount of flexibility desired are some of the criteria that need to

be considered when establishing the legal framework surrounding the formal depth of a relationship. It is up to the different stakeholders and eventually up to any overarching authority (such as the Federal Government) to determine which form fits best [29].

3.6.3 Joint Planning, Training, and Procurement

Many examples of joint initiatives in the fields of planning, training, and procurement can be given, some of which have previously been mentioned within the context of the 'Belgian CA' and the crisis management architecture. As such, the most far-reaching initiatives take place between the Ministry of Defence and the FPS Interior, notably within the structure of the Policy Board FedPol (Federal Police) which is a coordination organ between the Vice Chief Of Defence (VCHOD) and the Director General of the Federal Police. Discussions within this structure include topics such as the MIK, the NASC, use of UAS, the CBRNe platform, helicopter operations, and ongoing collaboration between the Military (SFG) and Police Special Forces (DSU) units. Within this organ, collaboration is being developed along five axis including operations, material resources, personnel resources, intelligence, and health and well-being. Within the HR axis, joint training mechanisms exist in various fields including police and military K-9 training, Explosive Risk Education (ERE), high-speed car handling, VIP protection (DAB) and (military) police motorcycle training. The aim within the HR axis is also to optimize the flow of personnel from one department to the other, notably the outflow of military personnel to the Federal Police for the purpose of VIP protection. The aim of the MR axis is precisely to permit joint procurement, promote synergies and interoperability, and to exchange best practices regarding public contracting. Ongoing initiatives include joint procurement of ballistic protection equipment, helmets, firearms, munitions, and specialised engineering vehicles. Although most of these initiatives are nascent, small-scale, police-military centric, and mostly bottom-up in nature, they have trickled up within the respective administrations to at least the DG level. The objective of the Policy Board is to widen the collaboration to at least other stakeholders within the FPS Interior being Firefighters and Civil Protection (besides the Federal Police).

In parallel, there is also a formal effort since July 2018 to promote multidisciplinary concertation and projects amongst several stakeholders being the Federal Police (including the underlying administrative, scientific, Disaster Victim Identification or DVI, DSU, and Air Support or DAFA services), the FPS Public Health (including the underlying security of the supply chain and the environment directorate, Emergency Medical Help directorate or DGH, and Emergency Medical Team or EMT services) and the Ministry of Defence (including the underlying strategy or ACOS STRAT and Explosive Ordnance Removal or SEDEE/DOVO service) [39]. Subsequent to this effort, a series of projects have been identified pertaining to civil security of which the following six have been tagged as a priority. The Ministry of Defence participates within the first five:

- Optimization of the unsafe warning for responders on their way to a dangerous location (output: procedures, agreements, training, and exercises);
- Forensic and security awareness among (non-police) responders (output: multidisciplinary basic training);
- Multidisciplinary "base camp" for operations and coordination/command (output: standards, modular elements and multidisciplinary Service Level Agreements or SLA);
- Operationalisation of the Emergency and Intervention Plans (Bijzonder Nood en InterventiePlan or BNIPs) with respect to the specific approach in cases of mass casualties (output: multidisciplinary operational doctrine, field tests and exercises);
- Availability of real-time images of incidents and interventions (output: practical analysis and tests, scenarios, users, agreements, and technology); and
- Multidisciplinary operational training for (deputy) directors of the disciplines (output: multidisciplinary training and exercises) [38].

Other projects identified within this initiative that are interesting from a CA perspective and require participation from the Ministry of Defence include projects linked to HNS, CBRNe, and terrorism.

At this time, however, most mature joint initiatives exist within the context of major international equipment programs and capability generation initiatives. Perhaps no better examples other than the Belgian-Dutch naval cooperation and Benelux initiatives exist to illustrate the will, ability, and limitations of the Belgian Defence with respect to joint planning, training, and procurement. As such, the Belgian-Dutch naval cooperation is seen as one of the best examples in the field of European defence cooperation [63]. This cooperation consists of a binational collaborative structure with the operational pillars of both Navies integrated into a single binational staff called Admiral Benelux (ABNL) [63]. The Dutch Naval Force Commander is the head of the ABNL, and his deputy is the commander of the Belgian Navy. The ABNL headquarters is located in Den Helder in The Netherlands. Making the staff binational means that each position within the staff can be filled by personnel from any of the two countries and that each person works for the whole [61]. This bi-nationalisation is not only limited to the staff; procurement of frigates, procurement of mine fighting vessels, logistical support, training and some of the naval schools such as the mine warfare school, the catering school and the frigate school have all been transformed into binational endeavours. Deployments and conduct of operations however always take place under national command. In doing so, both countries retain their sovereignty whilst joint procurement, maintenance and training enables the generation of a given level of military capabilities despite limited personnel and financial resources. Building on the success of this initiative, new impetus for greater Benelux defence cooperation came in 2012 with the 'Benelux Declaration on Defence Cooperation' signed by the Ministers of Defence of Belgium, Luxembourg, and the Netherlands [5]. This declaration established the politico-military Benelux Steering Group (BSG) under the three Ministers of Defence. For day-to-day coordination, the BSG is assisted by the Benelux Coordination Staff (BCS) and several Benelux Sub-Steering Groups (BSSG). There is a BSSG for each service or component i.e., BSSG Land, BSSG Navy, BSSG Air and BSSG Medical. This structure has enabled successful integration initiatives across a wide spectrum of military activities. First, one of the major achievements is in the field of airspace surveillance (QRA), where Belgium and the Netherlands both take turns to monitor and police the entire Benelux airspace. Second, there is close cooperation between Belgium and Luxembourg with regard to the acquisition, co-location, maintenance and training of the A400M and crew. Third, as far as the Army is concerned, the three countries cooperate in the Very high readiness Joint Task Force (VJTF) and are looking to strengthen cooperation between the Belgian and Dutch paratrooper schools [29]. Fourth, in the medical domain, there is an agreement to cooperate in terms of training and in terms of international postings [29]. Finally, yet importantly, a MoU was signed in 2014 for the establishment of the Benelux Arms Control Agency (BACA). This united the three national arms control and verification agencies into a single agency. Notably, for inspections and evaluations, Benelux is now considered as one State [29]. Again, as with the binational naval cooperation, Benelux joint planning, training, and procurement initiatives ensures greater cost efficiency and better resource utilisation. The interoperability between the three countries is also strengthened, as is the coordination at the policy level [5].

3.6.4 Standing Operating Procedures (SOPs), Equipment Compatibility, and Interoperability

Using the same equipment, sharing logistical support systems, joint structures, co-location, joint training, and joint exercises contributes to rendering units and capabilities compatible and interoperable. Examples range from those previously given within the Benelux context to F-16 fighter jets and C-130 transport airplanes. In such cases SOP's, radios, frequency channels, fuel standards and power plugs are very often the same. This state of affairs within the Benelux is expected to continue into the future given common upcoming platforms and programs such as the F-35 fighter jets, the Medium Range Transport Tanker (MRTT), Intelligence Surveillance Target Acquisition and Reconnaissance Systems (ISTAR), frigates, and counter-mine vessels. With the progress in implementation of the CaMo Project, the same can be said about future land systems [23]. Outside the mentioned frameworks, when countries do not share equipment, SOP's, compatibility, and interoperability are usually defined based on NATO standards.

In the field of interdepartmental compatibility and interoperability, several structures, systems, and platforms (such as MIK and SAR helicopters) have been previously mentioned that were specifically established, built, purchased, or equipped for compatibility and interoperability between military and civilian users. Interoperability and equipment compatibility of complex systems cannot be simply assumed; however, and this has to be examined on a case-to-case basis. As such, one of the most mature initiatives is the one taking place within the preview of the CBRNe platform and the NCC's interdepartmental workgroup for the operationalisation of CBRN emergency plans [57]. At this time, joint and standardised training (including a syllabus with common terminology) is being provided to a variety of first responders including military, police, firefighting, and medical evacuation personnel. The end objective is to foresee common equipment and procedures. This will enable all actors involved to be interoperable and to speak a common language during crisis response and judicial investigations in the field of CBRN events. Another mature initiative is the BGT or Basic Generic Training organised by the Egmont Institute[7] primarily to the benefit of the FPS FA. Under the BGT, Pre-Deployment Training (PDT) is provided to Belgian appointees travelling abroad for the purpose of civil crisis response operations. The end objective pertaining to this initiative is the promotion of common terminology and procedures. Within this program, the Ministry of Defence is involved in such courses are map reading, Explosive Risk Education (ERE), and radio procedures. Other less mature initiatives than the CBRNe and BGT initiatives also exist. Such is the case of the Police (DSU) and military (SFG) Special Forces units for example who intend to increase interoperability and develop common vectors and procedures despite facing mandate-relating restrictions and challenges.

3.6.5 Challenges to CA Implementation

Many generic challenges exist hindering collaboration across organisational boundaries. In the field of CA, partners are extremely diverse in terms of goals, structures, working practices and domains of activity. Domains of activity include military operations, humanitarian aid, human rights, protection of minorities, refugees and displaced persons, legal assistance, policing, firefighting, civil protection, medical care, reconstruction, and general project funding [29], [58]. With each organisation having its unique identity and culture, it is challenging for defence organisations to fully understand and master the complex stakeholder landscape. The Belgian Defence is equally exposed to this stakeholder complexity and the challenge this constitutes to further CA development. Some factors may be more pronounced within the Belgian context however (such as the lack of political continuity) while other factors may be mitigated by circumstances (such as the knowledge of many languages by most staff-level personnel). In general, one can broadly categorise these factors as hard factors and soft factors [20].

3.6.5.1 Structural or Hard Factors Identified within the Belgian Context

Several hard or structural factors were identified during our study. First, The Federal Government in Belgium is often characterised by unstable coalitions. This makes it difficult to achieve political unity and maintain this unity for more than the short term. Long-term vision and strategy development are thereby impaired [35]. In the fragmented Belgian political landscape, different political parties first have to compromise on their individual political agenda' without which no common vision can be realised, and no strong relationships can be established [20]. Once taken, decisions also have to stand longer than a single legislative term and not be reversed by the next Government [72]. Second and as in other countries, many CA-related decisions and options raise questions relating to sovereignty, control over resources, and control over decisions [30]. Third, even once a high-level political decision on collaboration has been taken, it is still hard to synchronise and harmonise decision making across stakeholders as reported by Heuninckx in the course of collaborations in major equipment projects [42]. In this regard, the establishment of the Policy Board FedPol also aims to open up procurement calendars amongst national partners. Ongoing discussions include the possibility for a joint helicopter platform between the police and military forces. Outside

[7] EGMONT – The Royal Institute for International Relations is an independent think-tank based in Brussels conducting interdisciplinary research and providing analysis and policy options mainly pertaining to foreign policy.

the defence and security sphere, a notable initiative to facilitate joint procurement and procurement planning is the Royal Decree on federally centralised procurement within the framework of the federal procurement policy of December 22, 2017 and the creation of a federal workgroup aiming to open federal tenders to other potentially interested parties [36]. Fourth, organisations may also have very different values and objectives within a partnership. For example, and as previously described, the DGDC, humanitarian organisations, and NGO's are very much attached to humanitarian principles (such as neutrality, impartiality and independence) which have proven sometimes difficult to reconcile with military logic in the past [29], [54]. In this regard much progress has been made over the last years through the different structures previously mentioned (TF, SG, …) as can be attested by such documents as the MoU with ENABEL and the DGDC's own strategy note [32]. The existence of discussions within these structures has also had a positive impact on such soft factors as confidence and trust amongst the partners as is discussed in the next paragraph.

3.6.5.2 Soft Factors Identified within the Belgian Context

Further, several soft factors were identified possibly impacting CA within the Belgian context. First, there may be big differences between partners with regard to term visions. For example, the DGDC may have a longer-term vision for projects as compared to the Ministry of Defence and the FPS FA who are mainly focused on responding to crises [36]. Second, the various departments may be "speaking" a different language. For example, the Ministry of Defence, as in other NATO military organisations, is characterised by a world full of abbreviations and specific terms which may not be understood outside the organisation [20]. In addition, neither Dutch nor French (which are the two most widely spoken languages in Belgium) are able to adequately accommodate both concepts of safety and security. In effect, both concepts are represented by a single word i.e., "veiligheid" (Dutch) or "securité" (French). This induces confusion, interpretation, and weariness amongst stakeholders as to what is actually being discussed within the context of CA and security policy. This can be detrimental to collaboration in a world where the most important difference between a security incident and safety accident may be the intentional character in causing damage (material, victims, fragility…). In effect, safety-focused actors should be able to vision the nexus with security and inversely. Similarly, discussions pertaining to Total Defence may induce weariness amongst some actors that the issue at hand is being "militarized" by the similarly named Ministry of Defence i.e., "Defensie" (in Dutch) or "La Défense" (in French) instead of focusing on the defence of national interest and values and the defence of society. Third, the difference in the hierarchy of the various partners may also play a role. Defence organisations are characterised by a tall hierarchy with clear decision-making responsibilities whereas other governmental agencies tend to have a flatter structure and decision-making process [20]. NGOs have an even more decentralised structure, little hierarchy and may be making decisions based on consensus [54]. Fourth, many stakeholders lack knowledge about partner organisations (including their hierarchy and decision-making process) which contributes to a lack of trust and misconceptions [35], [54] even if progress is being made as described in the previous paragraph. Combined with some of the other cultural and structural issues previously mentioned, lack of knowledge makes cooperation difficult [2] as is illustrated by Das and Teng's Figure 3-5 on trust and control in strategic alliances [11]. Besides the lack of knowledge on partner organisations, there may also be a lack of knowledge within some stakeholders on the concept of CA itself. Combined with the terminology-related issues, this partly explains the varying amounts of enthusiasm for the concept across the different Belgian stakeholders [20]. In order to be able to work well together within a framework such as CA, it is therefore important to overcome some of these structural and cultural differences. According to Das and Teng, collaboration can arise when there is little trust if this is compensated by enough control mechanisms which generate sufficient confidence to collaborate [11]. Conversely, when there is a lot of trust between the partners, little control is needed. The question is how Belgian partners create trust and achieve a level of control that enables confidence in a collaboration, thereby leading to effective cooperation [73].

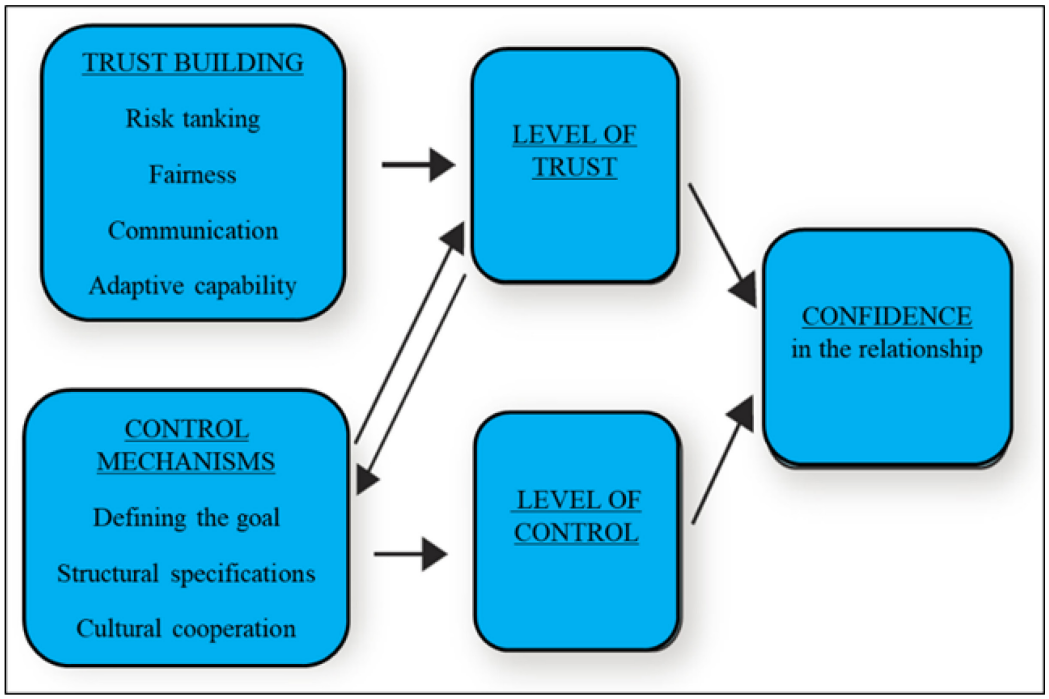

Figure 3-5: Trust and Control in Strategic Alliances, Adapted from Das and Teng [11].

One way forward to enhance trust is to improve strategic communication and to demonstrate flexibility towards partners. For example, flexibility can be demonstrated during harmonising of procedures and by enhancing transparency on goals and risks [54]. Strategic communication can be tailored to clarify terminology and to improve knowledge on the partner organisation, on the decision-making structure, and on the benefits of CA [20], [54], [58]. Enhancing communication and transparency also means that, besides sharing sufficient information, POC's need to be appointed for a long enough period so that trust can be established [73]. According to Decraene, knowledge could also be improved within the military itself through integration of adequate topics into Defence training courses [20]. Existing training programs can also be made more accessible to partners. For example, the Belgian Royal Higher Institute of Defence (or RHID) brings together top military and senior civil servants for a multidisciplinary course on security called the High Defence Studies Course. The civil servants need to have an explicit link with security or defence matters and are selected from various Public Services (FPS), International Organisations and civil society to include the economic, industrial, political, and academic world [45]. Finally, joint planning and the posting of embedded liaison officers at the highest levels across organisations are control and communication mechanisms that can contribute to effective strategic level relationships [58].

3.6.6 Societal Perceptions and Support

While the Benelux framework is sometimes compared to Nordefco or to Visegrad mechanisms, the application of a more society-centric approach such as Total Defence is a more challenging proposition within the Belgian context [29], [76]. Amongst other issues, not all stakeholders are ready for, or see benefit in extensive cooperation between defence and civilian organizations [76]. The context is therefore quite different from some other countries such as Norway where there is regular and active cooperation between the wider society and the military in the utilisation of resources and infrastructure [80]. At this moment in time, obtaining the support and confidence of the civilian population in terms of budget and recruitment to carry out core-organisational missions remains a key challenge from a Belgian Defence perspective [33]. Recent Defence contributions to anti-terror operations within the national territory as well as aid to the nation within the context of the COVID-19 pandemic have led to considerable improvement in the image and public support for Defence however [5], [33].

This is possibly due to the enhanced visibility of military units in the streets and within the media. According to Dumoulin, such visibility generates positive effects on recruitment as well as at the policy level where more attention and budgets can be obtained [33]. Having felt some benefits of enhanced visibility, the Ministry of Defence has now adapted its media and strategic communication philosophy. Within the Strategic Vision for Defence [22], the Belgian population is now earmarked as the main organisational stakeholder. All missions and tasks, for example the protection of Belgian nationals worldwide, are for its benefit [25]. The Mission Statement for Defence now also underlines the need to proactively communicate towards all stakeholders which is a departure from past tradition [29]. Accordingly, both the Policy Statement for Defence [26] and the Organisational Plan for Defence 2019-2020 [24] contain key communication related objectives [43].

In parallel to these changes, in 2018, the Ministry of Defence established a dedicated Strategic Communications Division (DG StratCom) incorporating a press service and taking over the responsibilities of spokesperson, crisis communication, operational communication, and strategic communication [21], [43]. The initiatives in the communication field aim to fulfil a number of sometimes interrelated objectives. First, the aim is to improve the recognition and the appreciation of the work of military personnel and thereby improve organisational identity [24]. Second, the aim is to improve and maintain a positive image for the Ministry of Defence as a whole [24]. Third, the aim is to demonstrate the importance of the organisation and improve knowledge on the organisation and the tasks it carries out, with respect to society [24]. In doing so, the intent is to increase the appeal of the military profession and to actively contribute to improving the organisation's recruitment efforts [24]. The intent is also to raise awareness as to the challenges encountered within in the field of defence and security, and to highlight the need for urgent and necessary investments in military capabilities [25]. Across initiatives, particular attention is given to the role of the media given the major role it plays in shaping stakeholder opinion and decisions [29], [33], [54], [58]

3.7 CONCLUSION AND RECOMMENDATIONS

3.7.1 Conclusion: State of Affairs in 2020

The Comprehensive Approach is not a question of one size fits all or 'everything or nothing': cooperation can take place at different levels and to various degrees. The variety in the level of implementation of CA within a country can be characterised by its breadth and its depth [66]. One measure of breadth is how comprehensive the National Security Strategy or similar doctrinal documents of the country are (number of actors, types of actors, …). Measures and instruments characterising the depth of relationships include the level of implementation in the legal hierarchy of documents (MoU, SOP), the type of joint equipment procurement, the level of cooperation between militaries in international operations, and qualitative assessments during joint crisis management exercises such as PACE18 and CMX [30]. When using these instruments to assess the state of CA in Belgium, it can be characterised as emergent. Whereas the CA Strategy Note [37] is undoubtedly an important step forward for Belgium in broadening interdepartmental cooperation, it also has very clear limits [29], [76]. For example, the approach is limited to the 3D-LO concept geared towards external crises, does not provide an answer to the nexus between internal and external safety and security, does not provide for formal reporting mechanisms to the Federal Government, and does not in itself contain any specific objectives and goals [20]. Pending a full-fledged National Security Strategy, different departments have to make ad hoc decisions and arrangements [72], [76]. This is a factor contributing to the difficulty in extending civil-military cooperation in Belgium to the level intended in concepts such as Total Defence. In addition, one may infer that Belgium has made substantial progress in the field of international cooperation, especially so within the contexts of the ABNL and Benelux frameworks. This also applies in certain aspects of interdepartmental cooperation such as the CBRNe platform and the Policy Board FedPol initiative. However, in such cases, the driver behind cooperation is not so much the political level but rather bottom-up enthusiasm from the administrative level [61]. Whether such bottom-up initiatives can form a strong enough power base to continue progress in the future in the absence of a NSS is still an open question. At this time, cooperation seems to occur when there is not much at stake, when the different actors are able to retain control of resources, and when

national or organisational sovereignty is preserved [30]. In the future, top-down vision, coordination and directives seem necessary to make hard decisions and to extend the depth of cooperation to such levels as task specialisation in capability generation and deployment [29], [61].

3.7.2 Recommendations and Future Developments

Whereas discussions within the Ministry of Defence seem to confirm the need for progress, and Belgian military staff (ACOS Strat) continues to actively contribute towards existing interdepartmental cooperation [24], convincing beyond the department remains challenging given the multiple soft and hard factors previously summarised. Several recommendations can be made in this regard. First, whereas the concept of CA in itself is beginning to take root in the national landscape under the impetus of supranational and bottom-up initiatives, there is still a need and room for more CA-linked terminology to trickle down in national documents. This includes terminology such as 'fragility' and 'resilience' as mentioned in the EU Global Strategy (2016) and NATO's concept of 'societal resilience'. At an individual level, it may be crucial that representatives clarify terminology and meaning behind some of the contested terms (security, safety, defence) before delving into the depth of discussions. Perhaps a positive contribution could be made if an independent academic body (such as the Egmont Institute or G4D for example) was to focus on a conceptual study to create a sort of 'linguae franca' across the multiple national stakeholders. Second, within the Ministry of Defence itself, the restructuring of Belgian military strategic communication efforts around the important organisations stakeholders and the media seems to be a step in the right direction. Discussion as to which crisis have to be solved by civilian authorities with military support and which crisis have to be solved by military authorities with civilian support need to be held [29]. Such a debate should be the culmination of a continuous effort to draft and maintain a National Security Strategy centred on national interests and values, risk assessment, scenario planning and operational plans. In the longer term, by impacting resources, processes, organisation structures, and the legal framework, the entire security architecture could be reviewed around a coherent National Security Strategy. Given the clear continuum between the internal and external aspects of CA, and the current fracture of CA in Belgium along an externally- and security-focused 'Belgian CA' on the one hand and an internally and safety-focused crisis management architecture on the other hand, SMEs from different fields need to further develop the nexus and linkages between the two into a coherent whole as part of this future NSS. Third, it may be that in the absence of a highly visible external threat to galvanise support from society, politicians, and the Government, bottom-up approaches within the context of existing structures may be the most promising way forward in the short term. For example, within the risk management task force of the CA SG, ongoing discussions concern the use of a joint risk management framework (such as FRAME or Fragility Resilience Assessment Management Exercise) to map the contextual and organisational risks within both the host and the donor country, to provide a 'common operational picture' facilitating interdepartmental cooperation, and to aid in the operationalisation of foreign policy [20], [35], [76]. Fourth, key budgetary and accountability obstacles to cooperation on CA projects need to be addressed similarly to what is being done on an EU level through Permanent Structured Cooperation EU (PESCO) and the European Defence Fund (EDF). As such, making money available for common projects seems to be a strong incentive. For example, one longer-term proposal to enhance interdepartmental cooperation in Belgium is the call for a common budget to finance actions within the framework of the 'Belgian CA' [35], [37]. Interestingly, more creative solutions have also been called for the financing of international collaboration and projects. The most noteworthy proposals include calls for better alignment of defence budget planning, new definitions of project cost-sharing formulas (such as GDP-based), harnessing of the previously mentioned PESCO and EDF, excluding collaborative procurement from EU convergence criteria, and VAT exemptions for collaborative programmes [42]. Finally but importantly, one must keep in mind that dwindling military and departmental resources which are often cited as the most important antecedent for collaboration is not the "raison d'être" of CA as such [5], [29], [42], [56], [63]. Rather, CA is the only solution to the fact that no actor, organisation or even country has sufficient means at its disposal to effectively navigate a major or complex crisis (as is continuously being demonstrated by the COVID-19 crisis). Thereby, collaboration between stakeholders with underlying C2 mechanisms, joint financing mechanisms, joint plans, and joint strategies are indispensable.

3.8 ACKNOWLEDGEMENT

First, we would like to thank Mr. William Demeyere who contributed to this study within the context of his master's thesis and thereby facilitated the generation of some of the insights presented in this chapter. Second, we would also like to acknowledge the comments and feedback received from two distinguished reviewers being Prof Ieva Berzina (Latvia) and Major Carl Decraene (Belgium).

3.9 REFERENCES

[1] Authelet, D. (2020), "Le SEDEE continue de travailler en période de coronavirus", Défense, Bruxelles, Belgique.

[2] Boogaerts, A. (2015), "De rol van burgers in defensie en de dagelijkse samenwerking tussen burgers en militairen in militaire organisaties", Koninklijke Militaire School, Brussel, België.

[3] Bouchez, G. (2020), "Outsourcing", Brussels, Belgium.

[4] Bries, R. (2017), "Capability development", Royal Military Academy, Brussels, Belgium.

[5] Coelmont, J. and Badot-Bertrand, H. (2019), "Interviews of Thys, M., Matthijssen, K. and Kalmes, Y.", Belgian Military Publication, Royal Higher Instiitute for Defense, Brussels, Belgium.

[6] Compernol, M. (2020), "Etat des lieux : que fait la défense dans la lutte contre COVID-19? Flash Défense, Défense, Bruxelles, Belgique.

[7] Cornille, L. (2014), "The deployment of cyber capabilities", Royal Military Academy, Brussels, Belgium.

[8] D'haene, G.J. (2020a), "COVID-19: Een logistieke puzzel", Defensie, Brussel, België.

[9] D'haene, G.J. (2020b), "Militairen nemen stalen af voor coronatests", Defensie, Brussel, België.

[10] Daems, I. (2014), "Pre-, during, and post-deployment psychological care for soldiers and their families in the Austrian and Belgian armed forces", Royal Military Academy, Brussels, Belgium.

[11] Das, T.K., and Teng, B.S. (1998), "Between trust and control: Developing confidence in partner cooperation in alliances", Academy of Management Review, Vol. 23 No. 3, pp. 491-512.

[12] Davis, R. (1992), "The foreign policymaking role of congress in the 1990s: Remote sensing technology and the future of congressional power", Congress and the Presidency, Vol. 19 No. 2, pp. 175-191.

[13] De Boeck J.M. (2020), "Defensie helpt sommige getroffen rusthuizen", Defensie, Brussel, België.

[14] De Croo A. (2020), "Accord De Gouvernement 30/09/2020", Chancellerie du Premier Ministre, Bruxelles, 2020.

[15] De Keermaker, J. (2020), "La composante médicale transporte les patients atteints du coronavirus entre les hôpitaux", Defense, Bruxelles, Belgique.

[16] De Keersmaker, J. (2020), "Militair hospitaal helpt sneller testen op coronavirus", Defensie, Brussel, België.

[17] De Kerchove, G., and Höhn, C. (2013), "Counter-terrorism and international law since 9/11, including in the EU-US context", Yearbook of International Humanitarian Law, Vol. 16, pp. 267-295.

[18] De Smet, H. (2020), "Civil-military crisis management", Interview by Demeyere, W., 29th April 2020.

[19] Debrackeler, J. (2020), "Les planificateurs médicaux, acteurs importants de la crise", Défense, Bruxelles, Belgique.

[20] Decraene, C. (2017), "Het concept 'fragiliteit' bij de planning en uitvoering van Belgische militaire operaties in het kader van een interdepartementale samenwerking", Koninkelijke Militaire School, Brussel, België.

[21] Decraene C. (2020), "ACOS Strat, integrated capability management, capability inform", Royal Military Academy, Brussels, Belgium.

[22] Defence (2016), "The strategic vision for defence", Defence, Brussels, Belgium.

[23] Defence (2017), "Land-med talks: Présentation projet capacité motorisée (CaMo)", Brussels, Belgium. 9 Jan 2017.

[24] Defence (2018), "The organizational plan for defence 2019 – 2022", Brussels, Belgium.

[25] Defence (2019), "The mission statement for the Belgian defence", Brussels, Belgium.

[26] Defence (2020a), "The policy handbook for defence", Brussels, Belgium.

[27] Defence (2020b), "La défense honore ses missions sur tous les fronts", Défense, Bruxelles, Belgique.

[28] Defence (2020c), "Follow-up COVID-19 on BEL areas of interest", Assistant Chief of Staff Operations and Training (ACOT), Brussels, Belgium.

[29] Demeyere, W. (2020), "Defense organisation stakeholders: Identification and management options", Royal Military Academy, Brussels, Belgium.

[30] Devries, S. (2014), "Europese defensie-samenwerking: Een exercicitie in de kantlijnen", Katern: Opninie, pp.10-14.

[31] Directorate General Development Cooperation (DGDC) (2014), "Strategy paper for humanitarian aid", Ministry of Foreign Affairs, Brussels, Belgium.

[32] Directorate General Development Cooperation (DGDC) (2019), "Policy framework for Belgian development cooperation in the security sector", Directorate General Development Cooperation, Brussels, Belgium.

[33] Dumoulin, A. (2017), "Défense citoyenne et citoyens de la défense : L'armée Belge et la Nation", Institut Royal Supérieur de Défense, Bruxelles, Belgique.

[34] European Defence Agency (EDA) (2019), "Military mobility fact sheet", European Defence Agency, Brussels, Belgium. https://www.eda.europa.eu/docs/default-source/eda-factsheets/2019-05-14-factsheet_military-mobility.pdf, consulted on 7th Sept 2019.

[35] L'Evêque, G. (2017), "Defence, diplomacy and development: The Belgian approach", Royal Military Academy, Brussels, Belgium.

[36] Federale Publiek Dienst Beleid en Ondersteuning (FPS Policy Support) or FPS BOSA (2017), "Koninklijk besluit inzake de federaal gecentraliseerde overheidsopdrachten in het kader van het federaal aankoopbeleid", Federale Overheidsdienst Beleid en Ondersteuning, 22 Dec 2017, https://www.ejustice.just.fgov.be/cgi/article_body.pl?language=nl&(...), Accessed Sep 14 2020.

[37] Federal Public Service of Foreign Affairs (FPS FA) (2017), "Strategic note on comprehensive approach: Note for the Council of Ministers", 20th July 2017, Brussels, Belgium, http://www.diplomatie.be/oda/comprehensive_approach_en.pdf., Accessed Sep 4 2020.

[38] Federal Publiek Dienst Binnenlandsezaken (or FPS Int) (2019a), "Werkingskader voor diverse projecten ter optimalisering van de multidisciplinaire operationele samenwerking bij grootschalige, complexe en langdurige incidenten", Federale Overheidsdienst Binnenlandse Zaken, Algemene Directie Civiele Veiligheid, May 17 2019.

[39] Goffin, P. and Compernol, M. (2020), Flash Défense, Défense, Bruxelles, Belgique.

[40] Governance for Development (or G4D) (2017), "Guidance on fragility", Governance for Development, Brussels, Belgium

[41] Governance for Development (or G4D) (2018), "A comprehensive approach for Belgian development cooperation", Governance for Development, Brussels, Belgium.

[42] Heuninckx, B. (2020), "International armaments cooperation", Royal Military Academy, Brussels, Belgium.

[43] Hart, G. (2020), "Strategic communication and media", E-mail Interview by Demeyere, W., Brussels, Belgium, May 8 2020.

[44] Hartley, T., and Russett, B. (1992), "Public opinion and the common defense: Who governs military spending in the United States?", American Political Science Review, 1992, pp. 905-915.

[45] Hautes Etudes de Sécurité et de Défense (HESD) (2019), "Brochure 2019", Institut Royal Supérieur de Défense, Bruxelles, Belgique.

[46] Hoslsag, J. (2019), "Security environment review", Belgian Defence. Brussels, Belgium.

[47] Iyengar, S., and Simon, A. (1993), "News coverage of the Gulf crisis and public opinion: A study of agenda-setting, priming, and framing", Communication Research, Vol. 20 No. 3, pp. 365-383.

[48] Kirton, J. (1993), "National mythology and media coverage: Mobilising consent for Canada's war in the Gulf", Political Communication, Vol. 10 No.4, pp. 425-441.

[49] Krosnick, J.A., and Brannon, L.A. (1993), "The impact of the Gulf War on the ingredients of presidential evaluations: Multidimensional effects of political involvement", American Political Science Review, 1993, pp. 963-975.

[50] Küsters, C. (2018), "Why is there no joint European remotely piloted aircraft system project under the common security and defence policy?", The RUSI Journal, pp. 52-65.

[51] Lasconjarias, G. (2017), "Deterrence through resilience: NATO, the nations and the challenges of being prepared", NATO Defense College, Research Division.

[52] Levy, Y. (2013), "How military recruitment affects collective action and its outcomes", International Studies Quarterly, Vol. 57 No. 1, pp. 28-40.

[53] Lievens, J. (2020), "Militair pompstation Melsbroek bevoorraadt luchthaven Luik", Defensie, Brussel, BelgIë.

[54] Luyckx, A. (2006), "Analyse van de synergieën tussen defensie en de NGO's in het geval van humanitaire crisissen", Koninklijke Miltaire School, Brussel, België.

[55] Mahon, T. (2015), "Cyber defence: Welcome to the next level", Warfare Concepts, Naval Forces, 1/2015, pp. 40-41.

[56] Møller, J.E. (2019), "Trilateral defence cooperation in the North: An assessment of interoperability between Norway, Sweden and Finland", Defence Studies. Vol. 19. No.3, pp.235-256.

[57] Nationaal Crisis Centrum (NCC) (2019), "Intense samenwerking voor chemische, biologische, radiologische en nucleaire risico's", Crisis Centrum, Brussel, België, 07 Juni 2019.

[58] NATO (2003), "NATO civil-military co-operation (CIMIC) doctrine", STANAG 2509/AJP-9.

[59] NATO (2019), "Performance management in defence organisations", SAS096, NATO Science and Technology Organisation, Paris, France.

[60] OESO (2016), "States of fragility 2016 report, brief No. 11", https://www.oecd.org/dac/governance-peace/publications/OECD%20States%20of%20Fragility%202016.pdf, Accessed Sep 14 2020.

[61] Parrein, P.-J. (2011), "De evolutie en toekomst van de Belgisch Nederlandse marinesamenwerking: Spill-over en politieke samenwerking", Koninklijk Hoger Instituut voor Defensie, Brussel, België.

[62] Raeymaekers, B. (2019), "Rapport d'activités 2018 : Un centre de crise interconnecté", Centre de Crise, Bruxelles, Belgique, Mar 5 2019.

[63] Sauer, T. (2015), "Deep cooperation by Belgian defence: Absorbing the impact of declining defense budgets", Defence Studies, Vol. 15 No. 1, pp.46-62.

[64] Scraeyen, L. (2016), "België gewapend tegen het terrorisme? Een lezing van het fenomeen en zijn bestrijding: Strategieën en middelen", Koninklijk Hoger Instituut voor Defensie, Brussel, België.

[65] Service Publique Fédeéal Intérior (or FPS Int) (2019b), "Arrêté royal relatif à la planification d'urgence et la gestion de situations d'urgence à l'échelon communal et provincial et au rôle des bourgmestres et des gouverneurs de province en cas d'événements et de situations de crise nécessitant une coordination ou une gestion à l'échelon national", Moniteur Belge, Bruxelles, Belgique, May 22 2019.

[66] Soares, J. (2020), "A literature review on comprehensive national defence systems", SAS152, NATO Science and Technology Organisation, Paris, France.

[67] Sigelman, L., Lebovic, J., Wilcox, C., and Allsop, D. (1993), "As time goes by: Daily opinion change during the Persian Gulf crisis", Political Communication, Vol. 10 No. 4, pp. 353-367.

[68] Stroobants, J. (2020a), "Guerre contre les fake news en ces temps de coronavirus", Défense, Bruxelles, Belgique.

[69] Stroobants, J. (2020b), “Nieuw detachement vigilant guardian”, Defensie, Brussel, België.

[70] Thomas, P. (2020), “Provinciecommando ondersteunt ontsmetting van Gentse ambulances”, Defensie, Brussel, België.

[71] Tranfield, D., Denyer, D., and Smart, P. (2003), “Towards a methodology for developing evidence-informed management knowledge by means of systematic review”, British Journal of Management, Vol. 14 No. 3, pp. 207-222.

[72] Van Dyck, B. (2015), “The Belgian security strategy: Reseach and recommendations”, Royal Military Academy, Brussels, Belgium.

[73] Van Eyck, J. (2018), “De Belgische cyberdefensie: welke mogelijkheden voor een Europese samenwerking?”, Brussel, België.

[74] Vanden Broeck, J. (2020), “La caserne de Gavere devient un point de distribution logistique”, Défense, Bruxelles, Belgique.

[75] Verboven, S. (2020), “Niemand anders dan Defensie had dit kunnen doen”, Defensie, Brussel, België.

[76] Verburg, M. (2020), “Belgische comprehensive approach”, Interview door Demeyere, W., Brussel, België, 4 May 2020.

[77] Verwilligen, K. (2020), “Opdracht volbracht voor Belgische luchtpolitie”, Defensie, Brussel, België.

[78] Vogels, O. (2020a), “Infectieziektes aan boord van schepen”, Defensie, Brussel, België.

[79] Vogels, O. (2020b), “Marinebasis Sint-Kruis verdeelt beschermende kledij”, Defensie, Brussel, België.

[80] Wither, J.K. (2020), “Back to the future? Nordic total defence concepts”, Defence Studies, Vol. 20 No. 1, pp. 61-81.

[81] Ybarra, C., Bueno, I., Endregard, M., Blatny, J.M., Dugauquier, C., Dhermain, J., Petronio, G., Engman, L.K. (2009), “Counter biological and chemical terrorism”, FFI-rapport 2009/00492, Norwegian Defence Research Establishment, Norway.

Chapter 4 – ESTONIAN CASE STUDY

Aarne Ermus
Estonian Military Academy
ESTONIA

4.1 INTRODUCTION

The purpose of this case study is to describe the Estonian approach to a comprehensive national defence. Comprehensive defence is understood as situation involving the military either in lead or support role. The study describes the main principles of comprehensive defence in Estonia, roles, and responsibilities of different stakeholders in planning and executing the comprehensive defence as well some lessons learned from the process of implementing the concept. The study is based on open-source material.

4.2 THREAT PERCEPTION, NATIONAL OBJECTIVES AND PRIORITIES

4.2.1 Threat Perception

The Estonian National Security Concept (ENSC), approved by the Parliament in 2017, reflects the complexity and density of the international security environment. From a global perspective, ENSC addresses a number of unsolved conflicts, humanitarian crises, but also growing ideological and religious extremism. Emphasizing the different roots of the possible global crises, natural disasters, environmental pollution, spreading of infectious diseases are mentioned. The concept predicts that the number of conflicts in near proximity of Euro-Atlantic zone will not decrease. The immediate threats to Estonia's security are linked with the Russia's ambitions to re-establish itself as the global superpower. Beside the traditional political, diplomatic, informational, and economical means, Russia is more inclined to use military power to achieve its objectives.

At the same time, there will be more sources of different complex threats: economic instability, developments in the cyberspace, technology-related threats, political radicalization, terrorism, organised crime, migration flows and variety of emergencies, like possible natural disasters, spread of infectious diseases or epizootics [18].

The Estonian National Defence Development Plan 2017 – 2026 (ENDDP-2017-2026) contains a more detailed and specific threat analysis part, but as a restricted access document, it is not part of this study.

4.2.2 National Objectives

The main objective of the security policy is described as "to secure the Nation's independence and sovereignty, the survival of the people and the state, territorial integrity, constitutional order and the safety of the population" ([18] p.2).

To be ready for complex threats and uncertainties, Estonia is implementing a broad approach to security and is following the comprehensive national defence concept. It is assumed, that only a combined application of diplomatic, informational, military, economic and social measures can create a sufficient deterrence to prevent the attack against the state and maintain the stability.

ENDDP-2017-2026 identifies the main objective of the plan as: "…to prevent and mitigate threats and tensions related to national defence, increase the deterrence against the possible military aggressor, faster development of the country's independent defence capability, rapid reaction to defence related crises and conflicts, and ability to resist attack by all means of society, increasing the cohesion of Estonian society and ensuring readiness to resist the information war" [17].

ENDDP-2016-2026 posits that defence related crises consist not only of military threats, but also emergencies and threats to the constitutional order of the state. Both strategic guidance documents approach national defence from a wider perspective than just military defence.

4.2.3 Principles

ENSC also identifies the main principles to achieve the security policy objective. These are:

- Estonian security policy is based on a broad security concept. Broad security is understood as the ability of a state and its people to defend intrinsic values and objectives from various external and internal political, military, economic and social threats and risks and their combined impact, as well as the capability to neutralize those threats and risks. In order to achieve this, national and non-state bodies and resources that have participated in shaping and maintaining a stable and peaceful environment are employed in a coordinated manner [18].
- Society as a whole and government as whole. Estonian security is strengthened by a cohesive civil society, in which its citizens' awareness and activity plays an important role in promoting security and safety. Estonia's security is strongest in a tolerant, caring, and participatory society [18].
- Comprehensive national defence. ENSC as well the ENDDP-2016-2026 do not provide a clear and precise definition of comprehensive defence but emphasize the use of military and non-military capabilities, activities and resources from the public and private sectors and civil society to defend the state.
- Estonia regards its own security and that of its allies as indivisible: the factors that influence the security of allies also affect Estonia and vice versa. Estonia contributes to NATO and the EU, in order to strengthen the solidarity of member states, counter the security threats in different regions, and improve the defence capability of member states [18].
- To maintain national sovereignty and its continuity, the goal of Estonian security policy is to prevent and pre-empt threats, as well as counter them quickly and flexibly, should the need arise. Estonia will defend itself in any case, no matter how overwhelming the opponent might be. If the state temporarily loses control over a part of its territory, Estonian citizens will engage in organised resistance in that area.

In planning the development of comprehensive defence for the ten-year period Estonia applies the following principles:

- The capabilities must be created in response to threat scenarios – military as well as non-military;
- The capabilities must be realistic and affordable;
- The capabilities created must ensure credible deterrence against the military aggressor; and
- Existing resources must be used efficiently, and sustainable capacity must be maintained [17].

The ENSC identifies the six main pillars of the comprehensive national defence [18]:

- Military defence;
- The civilian support to the military defence;
- International actions;
- Domestic and internal security;
- Maintenance of the uninterrupted functioning of the state and society; and
- Psychological defence.

The ENDDP-2016-2026 identifies six main lines of activities in the development of comprehensive defence:

- **Sustainability of the State and Society.** This line includes the functioning of the state and society by ensuring the continuity of vital services or other services essential for national defence under all circumstances. It also includes the execution of its main tasks by public authorities, the risk assurance and agility of public administration, and the strategic level crisis management capacity [17].
- **International activities.** This line includes the prevention and reduction of tensions at international level and the creation of appropriate conditions for both credible deterrence and the implementation of collective defence and crisis management. These activities are focused to provide Estonia with the favourable conditions that are necessary to help to implement effectively NATO's collective defence or international crisis management. International action also seeks to ensure that, in the event of a crisis or armed conflict, there is solidarity and a common understanding of the situation between NATO and the Member States of the European Union [17].
- **Strategic communication.** This line includes the development of national strategic communications and psychological protection. The purpose of strategic communication is to ensure support for Estonian security policy, to maintain public awareness of the security situation and to prevent panic, to neutralize hostile influence and to expose false information and prevent its spread. Strategic communication involves planning and consolidating the state's activities into one communicative entity and transmitting it to society [17].
- **Internal security.** This line includes ensuring internal security and the readiness of state institutions during a crisis or attack, as well as protecting Estonia's independence, sovereignty, and constitutional order. Ensuring internal security ensures the prevention of any covert or hybrid activities directed against the constitutional order of Estonia, as well as the protection of public order. In the event of an attack on Estonia, the fulfilment of the main tasks of the agencies, the availability of the necessary assistance to the residents or the resolution of the accompanying crises is ensured [17].
- **Civilian support to military defence.** This line includes the mobilisation of reserves and other state and non-state assets, reception of allied troops and support to them with the necessary infrastructure and goods. Furthermore, the line includes the assignment of defence related tasks to civilian service providers and implementation of these tasks through the establishment of contractual relations between the state and respective service providers [17].
- **Military defence.** This line includes the development and provision of self-defence capabilities and the implementation of NATO's collective defence. Estonia's military defence is based on independent defence capabilities and NATO's collective defence. Military defence provides sufficient capabilities to guarantee national sovereignty and to prevent, deter and repel military attack [17].

4.2.4 Priorities

These different capability development and action lines are not prioritised relative to each other. In addition to an overall objective, every activity line has its own, more specific sub-objectives. These objectives are described in a classified part of the document. In the publicly releasable part of the ENDDP-2017-2026, there is broad prioritisation, based on risk levels of different threat scenarios.

4.3 REFERENCES TO THE CONCEPT OF COMPREHENSIVE DEFENCE IN NATIONAL STRATEGIC DOCUMENTS AND LEGISLATION

4.3.1 Doctrinal Base and Plans

In basic terms, comprehensive defence relies on tight cooperation between different state agencies. To make such cooperation effective and efficient, several key conditions must be met. First, there should be common understanding about the comprehensive defence. Second, there must be clear understanding about each other's capabilities and sufficient interoperability in using these capabilities. Third, there must be joint contingency and action planning. Fourth, the state's legal system must enable such cooperation.

The Estonian National Security Strategy (ENSC) is the key document for building up common understanding at the strategic level. The last version of the strategy, emphasizing the broad security concept and comprehensive defence, was approved by the Parliament in 2017. It is the main framework document, to be taken account by all state policy sectors when drafting development and action plans. The strategy was prepared by the Government Office with the active participation of Ministries of Defence, Foreign Affairs, Internal Affairs, Economic Affairs and Communications, Social Affairs, Environment, and Finances. Therefore, as all the key ministries were involved into a process, the common understanding was built during the drafting of the strategy.

The Estonian State Defence Development Plan (ESDDP) is the overarching long-term development plan for the comprehensive defence. ESDDP describes what kind of military and non-military capabilities will be developed within ten-year timeframe to achieve the goals described in the National Security Concept. The plan is reviewed and updated every four years. The current ESDDP covers the period from 2017 to 2026, and the Government is preparing the new plan to cover the period 2021 – 2030. Formerly, the ESDDP was a plan only for the development of military capabilities. In 2013 capabilities to support the military were added for the first time and from 2017 the ESDDP gives the guidelines for the development of international activities, domestic security, and continuity of vital services as well for psychological defence.

The ESDDP 2017 – 2026 is linked with 18 different policy documents, state level development and action plans (see Appendix 4-1). All these plans and policy documents cannot be directly divided between the pillars provided in NSC or NDDP 2017 – 2026; there are overlaps and gaps. The responsibility for planning and development of these pillars lies with the respective ministries. The Ministry of Defence is responsible for the plans related to military defence and civilian support to the military defence. The Ministry of Foreign Affairs is responsible for the plans on international actions. The Ministry of Internal Affairs is responsible for the plans related to the internal security and sustainability of vital services. The Government Office is responsible for the plans on strategic communication and psychological defence. Of those, only Ministry of Defence has long practice in systematic capability planning which links 10-year plan to a 4-year mid-term, and 1-year short-term plans.

4.3.2 Legal Base

The main legal acts, framing the state defence and crisis management are:

- The Constitution of the Republic of Estonia;
- The National Defence Act;
- National Defence Duties Act;
- State of Emergency Act;
- Emergency Act;

- Law Enforcement Act;
- Estonian Defence Forces Organisation Act;
- Estonian Defence League Act;
- Police and Border Guard Act; and
- Rescue Act.

The Constitution of the Republic of Estonia gives the right to declare the state of war and state of emergency, also to order the mobilisation and demobilisation to the Parliament of the Republic (on the proposal of the President). The Parliament also decides the use of EDF to fulfil the international obligations of the Estonian Government. In certain cases, described in the constitution, the President has authority to declare the state of war or state of emergency [19].

The National Defence Act provides the legal framework for the peace-time and war-time national defence system; the management of mobilisation and demobilisation; the participation of the Republic of Estonia in the international military cooperation and the protection of national defence assets [24].

It clarifies the roles and responsibilities of the National Defence Council as an advisory body to the President of Republic and Security Committee of Government as the main coordinating body for the executive power in planning and executing the national defence tasks.

It also gives the coordinating authority for preparing national defence strategic documents and national defence action plans to the Government Office. The Government Office also has supervisory powers over the performance of the objectives determined in these documents. Thereby, at the level of strategic planning, coordinating mechanisms and tools are in place to ensure the unity of effort in planning the development of comprehensive national defence.

The Act also describes different defence readiness levels and specifies the changes in command authorities for the Prime Minister, CHOD, and Minister of Defence.

The Act establishes the legal framework for the international military cooperation and participation of EDF in international military operations. It is also the key act for regulating the arrival, stay and status of foreign military units on the territory of Estonia.

To ensure civilian support to the military defence, the act also regulates the assignment of defence tasks and work obligations when the different defence readiness levels are applied.

The Estonian Defence Forces Organization Act provides for the legal status and functions of the Estonian Defence Forces (EDF), the organisation of the EDF, the command authority and its limits for commanding the Defence Forces and the legal rules for the use of force by the Defence Forces [22].

This act defines the main tasks of the EDF: military defence of the state and participation in collective self-defence; preparation for the military defence and participation in collective self-defence; participation in military cooperation. From the point of view of comprehensive defence and crisis management it is important that the Act also regulates the military support to other agencies.

The Act identifies two main sets of conditions for the use of military forces:

- With the right to apply the force.
- Without the right to apply the force.

With the right to apply the force, the EDF can be used to support the police in the prevention and repelling of an attack against the national defence objects, and in preventing illegal border crossing and criminal offences. During the state of emergency, the EDF can be used with the right to apply force in preventing and repelling an attack against the governmental and defence installations, and in resolving emergency situations pursuant to the procedure provided for in the State Emergency Act.

Without the right to apply force, the EDF can be involved in responding to emergency and rescue works and to supporting police-on-police duties.

The use of the EDF is allowed only if the relevant authority cannot perform its functions in a timely manner or at all and there are no other means for performing such functions.

The relevant procedures on involvement of the EDF and EDL to support the Police and the Rescue Board are established by the Governmental decree on 28th June 2017.

The Emergency Act provides the legal basis for crisis management, including preparing for and resolving an emergency as well as ensuring the continuity of vital services. This Act also governs the declaration, resolution and termination of an emergency situation, the involvement of the Defence Forces and the Defence League in resolving an emergency that has led to the declaration of an emergency situation, and state supervision and liability. This Act does not govern preparing for combating a threat to national security or the constitutional order [30].

The State of Emergency Act provides the principles, conditions, and procedure for the elimination of a threat to the constitutional order of Estonia. It defines the main possible threats for the constitutional order: an attempt to overthrow the constitutional order of Estonia by violence; terrorist activity, collective violent oppression, extensive conflict between groups of persons involving violence, forceful isolation of an area of the Republic of Estonia, prolonged violent civil unrest [32].

The use of EDF and EDL under this act is limited to:

- Protection of public authorities and national defence infrastructure and assets against the possible attacks and prevention of such activities.
- Prevention of unlawful activity arising from collective violent oppression or from an extensive conflict between groups of persons involving violence;
- Prevention and resolution of unlawful activity involving forceful isolation of an area of the Republic of Estonia; and
- Prevention and resolution of a mass disorder involving violence.

The EDF and EDL can be used for these duties by the decision of the Government and approval of the President of the Republic. The Minister, responsible for the internal security, should make the proposal for such involvement and the Minister of Defence should approve the proposal.

The Law Enforcement Act provides the general principles of, basis for, and organisation of the protection of public order. This Act is not applied to the activity of the Defence Forces in the military defence of the state, in the preparation of military defence, in the performance of an international military obligation or in ensuring security of military infrastructure [31].

The Rescue Act provides the functions, organisation and rights of a rescue service agency, the involvement of the Defence Forces and the Defence League in the performance of the functions of a rescue service agency, and the rights and obligations of persons participating voluntarily in the activity of a rescue service agency [25].

4.3.3 Internal and International C2 and Logistical Interoperability

4.3.3.1 Any Existing Doctrinal Documents

In addition to the legal regulations and strategy documents, there are no existing overarching doctrinal documents on crisis management. The existing regulations are agency specific.

4.3.3.2 Organisational Setup Related to Civil-Military Crisis Management, to Include Provisions for Receiving and Providing International Support

The broad concept of crisis management in Estonia consists of three different types of crises regulated by different laws: The State Defence Act in a case of military threat; the State of Emergency Act in a case of threat against the constitutional order; and The Emergency Act in a case of different natural and manmade disasters (Table 4-1). Therefore, quite often terms as military and non-military crises are used.

In all cases, the overall responsibility for preparing for the crises and for resolving the crises lies with the Government and Prime Minister. Another commonality is that typically, there is a lead agency. The lead agencies responsible for planning the response and responding to the emergencies under The Emergency Act are assigned by the Governmental decree from 26th July 2018 as follows [21]:

- **Police and Border Guard**: The emergencies involving mass immigration of refugees, sudden attack, mass disorder or marine rescue event, including marine pollution.
- **The Rescue Board**: The emergencies involving flooding in densely populated areas, building fires with many victims and a major industrial accident.
- **The Environmental Board**: The emergencies involving radiation accidents.
- **The Health Board**: The emergencies related to mass poisoning and epidemics.
- **The State Information System Authority:** The emergencies related to the cyber-incidents.
- **Veterinary and Food Board**: The emergencies related to the animal diseases.
- If the **Security Police Board** has reasonable information to believe that the emergency was caused by terrorist activities, it has the right to take over the resolution of such emergency.

4.3.3.3 Roles and Responsibilities of Different Stakeholders

National security and defence issues, as well crisis management are dealt with in three strategic level meeting formats whose members occasionally overlap: The National Defence Council of the President; the National Security Committee of the Government; and the Crisis Committee of the Government.

The National Defence Council of the President discusses issues important to national defence and gives its opinion. The Council is the advisory body to the President and builds up consensus on security matters without any authoritative powers. Members of the Council are the Speaker of the Parliament, Prime Minister, the Chair of the National Defence Committee and the Chair of the Foreign Affairs Committee of the Parliament, the Ministers of Defence, Foreign Affairs, Finance, Interior, and Justice, Economic Affairs and Infrastructure and the Commander of the Defence Forces [24].

The National Security Committee of the Government has the central role in defence planning and execution at the strategic level. It is responsible for coordinating the activities of the state agencies on planning, developing, and executing the state defence and the activities of security services. The committee leads the process of preparing the National Security Strategy, National Defence Development Plans and National Defence Action plans. It assesses the national security situation and determines the need of the state for security-related information. It serves also as an advisory body for the government on security and defence

policy issues. The committee is comprised of eight ministers: the Prime Minister, and the Ministers of Defence, Foreign Affairs, Interior, Justice, Finance, Economy and Infrastructure, and Foreign Trade and Informational Technology [24], [23].

Table 4-1: The Types of the State Readiness.

Threat Situation			
EVENT • Accident; • Incident; • Managed by the responsible agencies.	**EMERGENCY** • Natural disaster; • Manmade disaster; • Interruption of vital services; • Epidemic; • Major accidents, which can't be solved without involving other partners, additional resources or changing the routine management lines.	**STATE OF EMERGENCY** • Threat to a constitutional order; • An attempt to overthrow the constitutional order of Estonia by violence; • Collective coercion involving violence; • Extensive conflict between groups of persons involving violence; • Forceful isolation of an area of the Republic.	**WAR** • Military attack against the state; or immediate threat of such attack.
–	**EMERGENCY SITUATION**	**STATE OF EMERGENCY**	**STATE OF WAR**
Legal Frame			
EMERGENCY ACT, RESCUE ACT, LAW ENFORCEMENT ACT		**STATE OF EMERGENCY ACT**	**THE NATIONAL DEFENCE ACT**

The Crisis Committee of the Government has the authority to coordinate the crisis management planning, development, and execution by government agencies. It has the legal right to assign tasks to the governmental agencies for the prevention and resolution of the emergencies. It also monitors the preparations for the emergencies by the respective agencies. If needed, the committee assists the authorities resolving an emergency of national impact or of particular severity, through the organisation of information exchange and coordination. The committee is led by the Minister of the Interior and is comprised of the Permanent Secretaries of all ministries (except the Ministry of Culture, and the Ministry of Science and Education). Members of the committee also include the Secretary of State, the Director General of the Rescue Board, the Chief of Staff of the Headquarters of the Defence Forces, the advisor to the Prime Minister for national defence issues, and other senior government officials [20].

The Government has the executive powers and responsibilities at the state level, to prepare for the emergencies and to react to them.

The Emergency Act defines an emergency as an event or a chain of events or an interruption of a vital service, which endangers the life or health of many people, causes major property or environmental damage, severe and extensive interferences with the continuity of vital services. The resolution of such events requires the coordinated activities between several agencies, the change in usual command lines and supplementary resourcing [30]. The right and the responsibility for identifying an event as an emergency lies with the respective agencies (Police and Border Guard, Rescue Board, Environmental Board, State Information System Authority, Veterinary and Food Board). To be able to manage the situation as an emergency, the government should declare the emergency by decree. Since 1991, this possibility was used only once, to respond to the COVID-19 virus. On 12th March 2020 the emergency situation on the territory of the Republic was declared by governmental order nr.76.

When declaring an emergency situation, the government appoints a leader of the emergency situation (usually the minister whose area of responsibility is affected) and also the leader of the emergency works from the respective agency. In the case of COVID-19, the Prime Minister was appointed as the leader of the emergency situation [26].

If EDF or EDL is required for the emergency work, the lead agency can directly ask for the support of the CHOD. If EDF or EDL is needed to help to secure the emergency area or to support law enforcement in the emergency area, a request for the support must be made by the respective ministry to a Government. The final decision in such cases is made by the President of the Republic. In both cases, CHOD will assign the selected unit under the tactical control of the person leading the resolution of the emergency. To respond the COVID-19, around 150 Defence League members were involved in temporary border control duties to support the Police and Border Guard from 15th March until 15th April 2020 [27]. The process was initiated by the Ministry of Internal Affairs, coordinated with the Ministry of Defence and approved by the President of the Republic before the governmental decree was published. All these approvals were made within one working day, which demonstrates the speed of the process.

The EDF and EDL were involved in the crisis response not only in a support role for the police. For example, the EDF field hospital was deployed to the island of Saaremaa to increase the local medical capabilities. In that case, formal procedure for the cross-service support was used (Health Care Agency requested support from the CHOD).

As the head of the emergency situation, the Prime Minister, using his order nr 38 from 17.03.2020, appointed four additional regional heads of the Rescue Service as regional heads of the emergency works. Their responsibilities were clarified within the same decree as follows:

- To coordinate the implementation of Governmental and Head of Emergency Situation decisions with municipalities;
- To coordinate the activities of state agencies and local municipalities in managing the crisis; and
- To coordinate the information exchange within the local municipalities [28].

In addition to these four appointed heads, the Prime Minister appointed by his order nr 43 20.03.2020, a fifth head of the emergency works (Minister of Public Administration), with the task of coordinating the provision of disinfectants and personal protective equipment to institutions and persons outside the health care and social welfare system [29].

Therefore, there were 6 different heads of emergency works involved, four with the regional responsibilities, and two within specific functional areas (The Health Care Agency was on lead in solving the core medical problem of the crisis).

It is clear that the strategic level crisis management with three different meeting formats (National Defence Council, National Security Committee and Crisis Committee) and two top level crisis management institutions (person in lead the emergency situation and person in lead of the emergency works) is top heavy, which may cause delay in real situation management. In addition, as there are no clear lines of responsibilities, it can be the possible cause of misunderstandings and contradictory decisions.

4.3.3.4 Standing Legal Provisions for Activation of the System and Further Escalation; Circumstances and Mechanisms by which Agencies Start Working Together, to Include International Cooperation

There are three separate legal processes in place to increase state readiness to counter the different crisis situations, regulated by different laws. Differentiation is based on threat types: military threat, threat to a constitutional order and threat of emergency (Table 4-1).

The National Defence Act defines four different levels of state defence readiness: general defence readiness, increased defence readiness, state of emergency, and war. These levels can gradually change depending on the level of threat to the security of state. Of these levels, the separate law (State of Emergency Act) regulates one: the state of emergency.

Even if there are no visible changes in the existing management and command system, every level of readiness consists of certain additional authorities for the Prime Minister, Chief of Defence and Ministry of Internal Affairs as well as limitations on executing their authorities for others.

4.4 CHALLENGES OF IMPLEMENTATION

4.4.1 Role of Organisational Culture and Institutional Barriers (to Include Budgets) in Enabling or Disabling Cross-Agency Cooperation

Evidently, the four main players in the crisis management system – the Defence Forces (including the Defence League), Police, Rescue Board and Health Board – have strong identities, traditions, and organisational culture. The way that members of these organisations see and interpret the world may cause misunderstandings during the joint operations. As was seen during common exercises, such differences can be overcome. At the same time, it is more difficult to build cooperation with agencies that do not have strong coherence and organisational culture.

In building cooperation and joint activities, one cannot miss the problem of the institutional barriers. On one hand, it is related to a habit of protecting valuable and sensitive information. On the other hand, it reflects the real world: all these agencies are also competitors for resources (finance, people, etc.). While EDF can be relatively certain on having 2% from GDP for the development and activities, there is no such certainty for other agencies. As there are no clear strategies on funding, these agencies face problems when it comes to a long-term perspective on resource planning.

4.4.2 Joint Planning, Training, and Procurement

From the joint planning perspective, the first step was made in developing the Estonian National Defence Plan 2017 – 2026. It harmonised the long-term objectives on the strategic level.

Estonia has a relatively long tradition of cooperation between four agencies (EDF and EDL, Police and Border Guard, Rescue Board and Health Board). The best examples are the participation of these agencies in the EDF exercise “Kevadtorm”. Also, EDL who has the main responsibility for the territorial defence is

organising smaller and bigger scale exercises also involving the Police, Rescue Board or Health Board. Participation in the exercises and training help to build up common understanding and between agencies and encourages them to learn from each other.

There is also limited educational cooperation. For example, the Estonian Military Academy and Estonian Academy of Security Sciences have conducted studies on crises management together. In addition, the Estonian Military Academy supports all universities in Estonia by providing training in war and disaster medical response.

Evidently, there are some examples of common procurement. For example, the EDF's last major small arms procurement project included the needs of the Police and Border Guard.

4.4.3 Standing Operating Procedures and Equipment Compatibility/Interoperability

In planning a response to possible events and reacting to emergencies, all agencies use their own SOPs, based on their knowledge and best practices. There is no common approach or set of standards in place that are accepted by everyone. Related to SOPs, another challenge is vocabulary. For every agency, the same terms may have the different meaning. The classical example is the word 'operation', which has a different meaning in military and in police. However, as ad hoc decision support structures (staffs) would be organised around the lead agency (which, in turn, depends on the nature of the emergency) and joined by the supporting agencies, a common SOP is crucial.

From the technical viewpoint, there are no major obstacles to cooperation. Because of the long practice of cooperation, agencies know each other's capabilities and limitations relatively well.

4.4.4 Societal Perceptions and Support

The civil protection concept, approved by the government in 2018 among other objectives, also refers to the need to increase the public's awareness about their own responsibilities and activities during different crises. The concept has three focus areas: teaching, civil defence and providing support. The concept refers to a study, commissioned by the Rescue Board in 2017, that found that people's overall knowledge about and readiness to cope emergencies is low. Therefore, as a possible tool to enhance the population preparedness for emergencies, the concept advises the inclusion of civil preparedness topics into a school curriculum during the next five-year period. The concept also advises an increase in civil defence related topics in the curriculum of "Defence Studies" for secondary school. From 2000, Estonian secondary schools have elective "Defence Studies" in their curricula. The subject is taught by active and reserve members of the EDF and EDL with the aim of increasing the students' security and defence related awareness.

Another tier of the same concept addresses the people's self-sustainability problems. Based on the same Rescue Board study from 2017, the authors concluded, that only 51% of the population has the required self-sustainability. From the point of the study, the accepted level of self-sustainability was ensured, if family had food supplies for one week, access to an autonomous water supply (a well, for example) and an alternative heating system. It is more difficult to meet such requirements in the cities than in rural areas.

The MOD of Estonia has been conducting the regular public opinion polls since 2001. The aim of these polls is to monitor public attitudes toward the national defence issues. With these polls MOD is collecting the information about:

- People's attitudes toward the Estonian state;
- The credibility of the state institutions (included defence structures);
- Assessments in connection with possible threats and security risks to Estonia and in the world;

- The will to protect the country and possible behaviour in the event of possible threats;
- Assessments of Estonia's defence capabilities and state's activities on developing these;
- Attitudes toward military service and other defence structures;
- Attitudes towards NATO and related developments; and
- Attitudes toward international military operations.

The Rescue Service, Police, EDF and EDL have been the most trusted institutions for a decade. The popular "will to defend" stays high. The passive "will to defend" stays at 80% from 2013. Of the male population, 75% (i.e., 78% of Estonians and 62% from other nationalities) is ready to participate actively in the defence of the country [33].

4.5 FUTURE DEVELOPMENTS, ONGOING DISCUSSIONS, AND PRELIMINARY CONCLUSIONS

Three years of implementing the new security strategy and NDDP has provided Estonia with some lessons learned. With the help of different exercises and wargaming, several weaknesses in the legislation have been identified [13]. The review process of the National Defence Act is ongoing. The process itself was initiated by the Government in 2016 and was led by the Ministry of Justice with participation of all affected ministries. As a result, the new proposals to change the National Defence Act were presented to a Parliament at the end of 2019.

The main findings of the review were following:

- There should be better harmony between broad security and comprehensive defence concepts and the state legislation. National Security Strategy declares that one of the objectives of the security policy is the safety of the population. Also, the ENDDP-2017-2026 covers this topic under the domestic and internal security pillar. At the same time, in the existing National Defence Act objectives of the national defence do not include the protection of the population. Therefore, the protection of the people would be added as the objective of the national defence into the law [13].
- In addition, the overall responsibility for crisis management development and action planning would be assigned to the Governmental Office. Until now, the responsibility was divided between the Governmental Office and the Ministry of Internal Affairs [13].
- Also, the existing legal construct, based on 3 different laws (The Emergency Act, The State of Emergency Act and The National Defence Act) is too sophisticated and does not ensure needed clarity and continuity in governance during crises [1]. Therefore, a proposal was made through the new law proposal, to discard the distinction between the State of Emergency and State of Defence.
- The Estonian comprehensive defence concept is relatively well developed at the strategic level through the existing National Security Strategy and overarching medium- and long-term development plans. The comprehensive defence is understood as a combined use of diplomatic, informational, military, economic and social measures to create the deterrence, to prevent the attack against the state and to defend the country.
- The lessons learned from the different wargaming and exercises helped to identify the shortcomings of the existing legal frame. Estonia is on its way to enhancing the existing legal framework to ensure that the needs of the comprehensive defence are better covered. The main emphasis is on the clarification of the roles and responsibilities of different stakeholders on crisis management and the simplification the crisis management system as a whole.

- Estonia has a solid practice of interagency cooperation in the practical solving of emergencies and the execution of joint exercises on different levels. To enhance this cooperation, the crisis management system may need standardised SOPs and a solid doctrinal base, even though ad hoc solutions have been working well.

4.6 REFERENCES

[1] Government of the Republic of Estonia (2019), "Explanatory memorandum Riigikaitseseaduse eelnõu seletuskiri", (English title: Explanatory memorandum to the State Defence Act) https://www.riigikogu.ee/tegevus/eelnoud/eelnou/94bd4697-41b5-4e9f-80f1-bda86715146e/Riigikaitseseadus.

[2] Ministry of Culture (2016), "Lõimuv Eesti 2020", (English title: Integrating Estonia 2020), https://www.kul.ee/sites/kulminn/files/le2020_arengukava_uuendatud_2016.pdf.

[3] Ministry of Defence (2010), "Eesti kui vastuvõtva riigi toetuse kontseptsioon", English title: Concept of Host Nation Support), https://www.riigiteataja.ee/aktilisa/3311/2201/0002/VVk_498_lisa.pdf#.

[4] Ministry of Economic Affairs and Communications (2013), "Transpordi Arengukava 2014 – 2020", (English title: National Transportation Development Plan 2014 – 2020), https://www.riigiteataja.ee/aktilisa/3210/2201/4001/arengukava.pdf.

[5] Ministry of Economic Affairs and Communications (2017), "Energiamajanduse arengukava", (English title: National Development Plan of the Energy Sector until 2030) https://www.mkm.ee/sites/default/files/enmak_2030.pdf.

[6] Ministry of Economic Affairs and Communications (2018), "Digital Agenda 2020 for Estonia", https://www.mkm.ee/sites/default/files/digitalagenda2020_final.pdf.

[7] Ministry of Economic Affairs and Communications (2018), "Estonian cyber security strategy 2019 – 2022," https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf.

[8] Ministry of Economic Affairs (2012), "Eesti merenduspoliitika 2012 – 2020", English title: Estonian Marine Policy 2012 – 2020), https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/eesti_merenduspoliitika_2012-2020.pdf.

[9] Ministry of Environment (2017), "Kiirgusohutuse riiklik tegevuskava 2018 – 2027," (English title: National Radiation Safety Development Plan 2018-2027) https://www.envir.ee/et/eesmargid-tegevused/kiirgus/kiirgusohutuse-riiklik-arengukava-2018-2027.

[10] Ministry of Finance (2013), "Üleriigiline planeering 2030+", (English title: Estonia 2030+), https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/eesti_2030.pdf.

[11] Ministry of Internal Affairs (2015), "Siseturvalisuse arengukava 2015 – 2020," (English title: The Internal Security Development plan 2015-2020), https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/taiendatud_siseturvalisuse_arengukava_2015-2020.pdf.

[12] Ministry of Internal Affairs (2018), "Elanikkonna kaitse kontseptsioon", (English title: The Civil Protection Concept) https://www.riigikantselei.ee/sites/default/files/content-editors/organisatsioon/failid/rakkeryhmad/elanikkonnakaitse_kontseptsioon_15.02.2018.pdf.

[13] Ministry of Justice (2018), "Working group report "Riigikaitseõiguse muudatuste kontseptsioon", (English title: Concept of changes in state defence legislation), https://www.just.ee/et/riigikaitseoiguse-revisjoni-valminud-materjalid.

[14] Ministry of Rural Affairs (2014), "Eesti maaelu arengukava", (English title: Estonia – Rural Development Programme (National)), https://www.agri.ee/et/eesmargid-tegevused/eesti-maaelu-arengukava-mak-2014-2020.

[15] Ministry of Social Affairs (2012), "The National Health Plan 2009 – 2020", https://www.sm.ee/sites/default/files/content-editors/eesmargid_ja_tegevused/Tervis/Aruanded/rta_2009-2020_2012_eng.pdf.

[16] Parliament of the Republic of Estonia (2005), "Estonian National Strategy on Sustainable Development "Sustainable Estonia 21", https://www.riigikantselei.ee/sites/default/files/content-editors/Failid/estonia_sds_2005.pdf.

[17] Ministry of Defence (2017), "National Defence Development Plan 2017-2026. Overview", https://kaitseministeerium.ee/sites/default/files/elfinder/article_files/rkak_2017_2026_avalik_osa.pdf (in Estonian).

[18] Ministry of Defence (2017), "National Security Concept of Estonia", https://www.kaitseministeerium.ee/en/objectives-activities/basic-national-defence-documents.

[19] Riigi Teataja (2015), "The Constitution of the Republic of Estonia", https://www.riigiteataja.ee/en/eli/521052015001/consolide.

[20] Riigi Teataja (2017), "Governmental decree Vabariigi Valitsuse määrus nr 111, 22 Jun 2017, Vabariigi Valitsuse kriisikomisjoni põhimäärus", (English title: Statute of the Crisis Committee of the Government), https://www.riigiteataja.ee/akt/128062017038.

[21] Riigi Teataja (2018), "Governmental decree nr. 63.from 26.07.2018, Vabariigi Valitsuse määrus nr 63 26 Jul 2018 Hädaolukorrad, mille kohta tuleb koostada nende lahendamise plaan ja mille puhul korraldada riskikommunikatsiooni, ning hädaolukordade lahendamist juhtivad asutused", (English title: Emergencies for which a contingency plan must be drawn up and for which risk communication must be carried out, and emergency management bodies), https://www.riigiteataja.ee/akt/131072018004.

[22] Riigi Teataja (2019), "Estonian Defence Forces Organisation Act", https://www.riigiteataja.ee/en/eli/503062019005/consolide.

[23] Riigi Teataja (2019), "Governmental decree Vabariigi Valitsuse määrus nr 129, 28 Jun 2019, Vabariigi Valitsuse julgeolekukomisjoni põhimäärus", (English title: Statute of the security committee of the Government.), https://www.riigiteataja.ee/akt/115122015006.

[24] Riigi Teataja (2019), "The National Defence Act", https://www.riigiteataja.ee/en/eli/502042019010/consolide.

[25] Riigi Teataja (2019), "The Rescue Act", https://www.riigiteataja.ee/en/eli/520032019001/consolide.

[26] Riigi Teataja (2020), "Governmental order Vabariigi Valitsuse korraldus nr, 76 12 Mar 2020, Eriolukorra väljakuulutamine Eesti Vabariigi haldusterritooriumil", (English title: Declaration of Emergncy Situation in the Administrative Territory of the Republic of Estonia.), https://www.riigiteataja.ee/akt/324042020007.

[27] Riigi Teataja (2020), "Governmental order Vabariigi Valitsuse korraldus nr 79, 17 Mar 2020, Kaitseliidu kaasamine avaliku korra kaitsesse eriolukorra ajal," (English title: Involvement of the Defence League in Protecting Public Order During Emergency Situation.), https://www.riigiteataja.ee/en/eli/518032020001/consolide.

[28] Riigi Teataja (2020), "Prime Minister of Estonia order no 38 Appointment of persons in charge of emergency situation work for coordinating compliance with orders and organizing SMS alerts", https://www.riigiteataja.ee/en/eli/521032020002/consolide.

[29] Riigi Teataja (2020), "Prime Minister of Estonia order no 48 20.03.2020. Peaministri 17. märtsi 2020. a korralduse nr 38 Eriolukorra tööde juhtide määramine korralduste täitmise koordineerimiseks ja SMS ohuteavituse korraldamiseks muutmine", https://www.riigiteataja.ee/akt/320032020002.

[30] Riigi Teataja (2020), "The Emergency Act", https://www.riigiteataja.ee/en/eli/516052020003/consolide.

[31] Riigi Teataja (2020), "The Law Enforcement Act", https://www.riigiteataja.ee/en/eli/508052020005/consolide.

[32] Riigi Teataja (2020), "The State of Emergency Act", https://www.riigiteataja.ee/en/eli/512052020002/consolide.

[33] Turu-uuringute, A.S. (2019), "Avalik arvamus ja riigikaitse. Sügis 2019. Turu-uuringute AS aruanne kaitseministeeriumile", (English title: Public opinion and state defence. Report for the Ministry of Defence.), https://www.kaitseministeerium.ee/sites/default/files/sisulehed/avalik_arvamus/aruanne_sygis_2019.pdf.

Appendix 4-1: THE MAIN CONCEPTUAL DOCUMENTS AND PLANS, LINKED WITH, OR INFLUENCING THE ENDDP-2017-2026

Table 4A1-1: The Main Conceptual Documents and Plans, Linked with, or Influencing the ENDDP-2017-2026.

No.	Title	Status	Type of Document	Owner	Approved by	Relevance to a NDDP
1	Estonian National Security Strategy	Approved by Parliamentary decision on 31.05.2017.	Policy document	GOV	PoE	Establishes the main objectives, principles and directions in security policy (including Comprehensive defence) [18].
2	Estonian National Strategy for Sustainable Development Sustainable Estonia"	Approved by Parliamentary decision on 14.05.2005.	State development strategy	GOV	PoE	Strategy focuses on the long-term sustainable development of the society. Cross-over areas: viability of the Estonian cultural space, the growth of well-being and cohesive society are connected with domestic and internal security and the Psychological defence pillars of the comprehensive defence [16].
3	The Internal Security Development plan 2015 – 2020	Approved by Governmental decree 17.11.2015. Under the revision. Will be replaced by the new development plan for the 2020 – 2030.	Development plan	MIA	GOV	Cross-over areas: development of the police and rescue board capabilities, crises prevention, emergency preparedness, border management and ensuring the security at the state border [11].
4	The Civil Protection Concept	Approved in 2018.	Policy document	MIA	GOV	Survivability of society; peoples readiness for the crisis sitations [12].
5	Estonian Cybersecurity Strategy 2019 – 2022	Approved in 2018.	Policy document	GOV	MEC	Cross-over areas: cyber defence, protection of vital services [7].

No.	Title	Status	Type of Document	Owner	Approved by	Relevance to a NDDP
6	National Radiation Safety Development Plan 2018 – 2027	Approved by the Minister of Environment in 2017.	Development plan	MOE	MOE	Linked with crisis and emergency management. Concerns roles and responsibilities of different actors to ensure preparedness for a radiological emergencies [9].
7	The National Health Plan 2009 – 2020	Approved by Government decree in 20.12.2012. Under revision. Will be replaced with the Plan for 2020 – 2030.	Development plan	MSA	GOV	Linked with the development and sustainabilities of the health care system. The development plan is aimed at building a safety network essential for the preservation of the independence of Estonia. Danger scenarios help determine the necessary military skills and resources for the development plan.[15].
8	Integrating Estonia 2020	Approved by government decree in 16.05.2016. Under the revision. Will be replaced with Integrating Estonia 2030.	Development plan	MOC	GOV	The state integration policy is necessary to ensure the sustainability of the Republic of Estonia. Comprehensive national defence requires greater cohesion in society in order to stand against the information war against Estonia and influencing activities [2].

No.	Title	Status	Type of Document	Owner	Approved by	Relevance to a NDDP
9	Estonian Marine Policy 2012 – 2020	Approved by Governmental decree in 02.08.2012. Under the revision. The new policy will be part of the transportation development plan.	Policy document/ development plan	MEC	GOV	From the point of view of national defence, the development of maritime safety and security is important in order to ensure the possibility of both the movement of Estonian units and the reception of allies [8].
10	National Transportation Development Plan 2014 – 2020	Approved by parliamentary decision in 19.02.2014. Under the revision.	Development plan	MEC	GOV	From the point of view of national defence, the field of transport development is important in order to ensure the possibility of the movement of Estonian units and the reception of allies, the use of alternative solutions for the transport of units and residents, as well as in the event of a crisis the possibility for the population to move safely from one area to another [4].
11	Digital Agenda 2020 for Estonia	Approved by the government decision in 2018.	Development plan	MEC	GOV	Within this framework, one of the sub-objectives of the plan is the creation of information and communication technology infrastructure supporting the development and well-being of the population, as well the economic growth and the state development. Such infrastructure is needed to better ensure the cohesion of society [6].

No.	Title	Status	Type of Document	Owner	Approved by	Relevance to a NDDP
12	Estonia 2030+	Approved by governmental decision in 30.08.2012.	Plan	MOF	GOV	The national spatial plan Estonia 2030+ consists of, among all other topics, development principles of Estonia's energy infrastructure. From the point of view of national defence, such an approach is also related vital services and the continuity of society [10].
13	Estonian Rural Development Plan 2014 – 2020	Approved by the government in 2014. No information available about the revision.	Development plan	MRA	GOV	Development plan activities are related to the food supply chain and risk management. The development plan also includes measures for sustainable food productionactivities. Such activities are related to ensuring food security [14].
14	National Development Plan of the Energy Sector until 2030	Approved by governmental decision in 2017.	Development plan	MEC	GOV	The development plan includes the measures to ensure a continuous energy supply to the population. In addition, the development plan highlights the measure to create and maintain fuel stocks. Therefore, it applies to vital services and continuity of society [5].
15	Concept of Host Nation Support	Approved by the Government in 23.12.2010.	Concept	MOD	GOV	Tasks and responsibilities of state agencies in providing Host Nation Support to the NATO units [3].

Appendix 4-2: THE MAIN STAKEHOLDERS AND THEIR RESPONSIBILITIES IN PREPARATION AND MANAGEMENT OF THE DIFFERENT CRISES

Table 4A2-1: The Main Stakeholders and Their Responsibilities in Preparation and Management of the Different Crises.

	Emergency Situation	State of Emergency	State of War
President of the Republic	Approves the use of the EDF or EDL on law enforcing functions during the crisis situation management.	Makes the written proposal to the Parliament to declare the State of Emergency.	Makes the proposal to the parliament to declare the state of war and to order the mobilisation or demobilisation. In a case of agressioon declares the war and mobilisation without waiting the Parliamentary resolution.
National Defence Council	-	Discuss the matters of significant importance to national defence and provides opinion on such matters.	Discuss the matters of significant importance to national defence and provides opinion on such matters.
Parliament of the Republic	-	Declares the State of Emergency.	Declares the State of war, mobilisation and demobilisation. Approves the government decision on increase of the defence readiness.
Government and Ministries			
Government of the Republic	Declares the emergency situation; Appoints the person in charge of emergency situation, who is typically one of ministries;	Makes the written proposal to the Parliament to declare the State of Emergency; Decides the involvement of EDF and EDL.	May issue administrative acts to organise or enhance defence readiness of the state and resolution of state of war which are indispensable for the rapid solution of threatening situation.

	Emergency Situation	State of Emergency	State of War
Prime Minister	-	The head of the state of emergency; Convenes a session of the Government of the Republic, during which the opinion of the Security Committee of the Government of the Republic on the need for the declaration of a state of emergency is heard.	Directs the organisation of increased defence readiness and handling the state of war. Gives orders to a respective ministries, agencies, and municipalities. May issue administrative acts to organise or enhance defence readiness of the state and resolution of state of war, which are indispensable for the rapid solution of threatening situation.
National Security Committee	Co-ordinates the activities of respective agencies in preparing for the crises and in execution of crisis management tasks.	Analysing and assessing the security situation; Co-ordinates the collection of information.	Coordinating the activities of respective ministries and agencies on preparing the strategic development and action plans for the state defence. Analysing and assessing the security situation. Co-ordinates the collection of information.
The Crisis Committee of the Government	Co-ordinates the activities of the respective agencies on planning, development and execution of crisis management tasks; Gives tasks to the respective agencies on prevention of emergencies; Assess the emergency situations and risks.	-	-

	Emergency Situation	State of Emergency	State of War
Government Office	Supports the planning of government's work; Organises public relations for the government; Advices the Prime Minister on national security; Manages the coordination of national security and defence management.	Supports the planning of government's work; Organises public relations for the government; Advices the Prime Minister on national security; Manages the coordination of national security and defence management.	Supports the planning of government's work. Organises public relations for the government. Advises the Prime Minister on national security. Manages the coordination of national security and defence management.
Ministry of Defence	Approves the involvement of the EDF and EDL.	Approves the involvement of the EDF and EDL.	Makes proposals to the Government to increase defence readiness.
Ministry of the Interior	After consulting with the Ministry of Defence, proposes to the government that it involve the EDF or EDL to resolve the emergency, in cases where the emergency falls into the field of responsibility of the respective ministry.	Makes proposals to involve the EDF and EDL to solve the situation; As the chief of internal defence, the minister of Interior leads the resolution of the situation.	May issue administrative acts to organise or enhance defence readiness of the state and resolution of state of war, which are indispensable for the rapid solution of threatening situation.
Ministry of Foreign Affairs	International activities.	International activities.	International activities.
Ministry of Finance			
Ministry of Economic Affairs and Communications	After consulting with the Ministry of Defence, proposes to the government that it involve the Defence Forces or Defence League to resolve the emergency, in cases where the emergency is falls into the field of responsibility of the respective ministry.		
Ministry of Justice			

	Emergency Situation	State of Emergency	State of War
Ministry of Social Affairs	After consulting with the Ministry of Defence, proposes to the government that it involve the Defence Forces or Defence League to resolve the emergency, in cases where the emergency is falls into the field of responsibility of the respective ministry..		
Ministry of Environment	After consulting with the Ministry of Defence, proposes to the government that it involve the EDF or EDL to resolve the emergency, in cases where the emergency falls into the field of responsibility of the respective ministry.		
Main Agencies Involved			
Chief of Defence Forces EDF	Supports the respective agencies with units, materials and equipment to solve the emergency.	Supports the respective agencies with units, materials and equipment to solve the emergency.	May issue administrative acts to organise or enhance defence readiness of the state and resolution of state of war, which are indispensable for the rapid solution of threatening situation.
EDL	Supports the respective agencies with units, materials and equipment to solve the emergency.	Supports the respective agencies with units, materials and equipment to solve the emergency.	
Police and Border Guard	Leads the resolution of emergencies in a case of mass immigration of refugees, in a case of sudden attack, mass disorder or in a case of marine rescue event, including the marine pollution.	Leads the resolution of emergencies in a case of mass immigration of refugees, in a case of sudden attack, mass disorder or in a case of marine rescue event, including the marine pollution.	

	Emergency Situation	State of Emergency	State of War
Security Police	Leads the resolution of emergencies in a case of terrorist activities.	Leads the resolution of emergencies in a case of terrorist activities.	
Rescue Board	Leads the resolution of emergencies in a case of flooding in densely populated areas, in a case of building fires with many victims and in a case of a major industrial accident.	Leads the resolution of emergencies in a case of flooding in densely populated areas, in a case of building fires with many victims and in a case of a major industrial accident.	Leads the resolution of emergencies in a case of flooding in densely populated areas, in a case of building fires with many victims and in a case of a major industrial accident.
Environmental Board	Leads the resolution of emergencies in a case of radiation accidents.		
Health Care Board	Leads the resolution of emergencies in a case of a mass poisoning and epidemics.		
Veterinary and Food Board	Leads the resolution of emergencies in a case of animal diseases.		
The State Information System Authority (RIA)	Leads the resolution of emergencies in a case of cyber-incidents.	Leads the resolution of emergencies in a case of cyber-incidents.	Leads the resolution of emergencies in a case of cyber-incidents.
Others			
Regional Crisis Committees	Co-ordinates the execution of the crisis management tasks by subunits of governmental agencies and municipal authorities in a specific region.	-	-
Local Crisis Committees	Co-ordinates the execution of crisis management tasks in municipality.	-	-

Chapter 5 – LATVIAN CASE STUDY

Ieva Berzina
National Defence Academy of Latvia
LATVIA

5.1 INTRODUCTION

The annexation of Crimea by Russia and the following war in Ukraine prompted Latvia to look for ways to strengthen self-defence capabilities because the contemporary conduct of warfare opens opportunities for circumventing the principles of collective security. The chosen option was the adaptation of the total defence concept to the circumstances of the 21st century. Due to the increasing use of non-military means for the achievement of political and military goals, it was decided to use the term "Comprehensive National Defence" (CND), which is broader in terms of the involved structures and dimensions of interaction with an adversary – military, civilian, informational, psychological, economic, diplomatic, and other. Latvia started to implement the CND system in 2018. The chapter describes and analyses the development of CND in Latvia from 2018 to 2020.

5.1.1 The Concept of CND in National Strategic Documents

In 2018 the Latvian Ministry of Defence prepared an informative report "On Implementation of Comprehensive National Defense System in Latvia" [20], which is an initial policy planning document and may be regarded as a point of reference for contemporary CND system implementation. The document defines the concept of the CND system, its goals, as well as short-, medium- and long-term tasks, and the key areas and institutions responsible for them. The document defines that "the key purpose of CND is to enhance Latvia's deterrence capabilities and build resilience against possible crises or armed conflicts" [35] (p.2). The informative report outlines seven key areas of Latvia's CND model, which may be "adjusted and expanded as necessary" (Table 5-1). Thus, the document provides a balanced basis for further action, covering military and non-military means of defence as well as hard and soft aspects of security. On January 8, 2019, the informative report was reviewed and supported by the Cabinet of Ministers.

The implementation of CND requires fundamental changes in Latvian society's approach to national security, which requires amendments to legislation. The National Security Law "prescribes the national security system and tasks of such, the competence of the persons or institutions responsible for the national security system and the principles and procedures of coordination, implementation, and control of their activities" [34] (Section 2). On October 4, 2018, several amendments in the National Security Law were adopted in connection with the implementation of CND. The Law now includes a section on CND (the official translation of the Law uses the term "Comprehensive State Defence"): "to provide comprehensive State defence in case of war, military aggression or occupation until the moment the authorities implementing legitimate State authority and administration are fully restored, the National Armed Forces, State administration and local government authorities and also natural and legal persons shall implement measures for military and civil protection of the State and conduct armed resistance, civil disobedience and non-cooperation with illegal administration authorities" [34] (Section 23.[5]).

The core idea of this amendment is resistance – it clearly defines that responsible institutions and society shall use all available means and resources to resist a military attack on state sovereignty. This is further clarified by the other amendments to the National Security Law adopted on October 4, 2018. The Law now has a Section on "Obligations and Rights of Citizens in Case of War or Military Aggression" that determines citizens' obligations: "to perform the tasks given by the National Armed Forces and the units of the armed forces of the North Atlantic Treaty Organization and European Union Member States providing assistance in

the performance of their tasks and ensuring military protection of Latvia, and also other State administration and local government authorities responsible for overcoming danger to the State" and "to not cooperate with illegal administration authorities and armed units of the aggressor, except when such refusal to cooperate endangers the life or freedom of the person or his or her family members" [34] (Section 25.[1](1)). The citizens also have the right to implement civil disobedience, to demonstrate armed resistance, and to support the members of civil disobedience and armed resistance, as well as national and Allied armed forces [34] (Section 25.[1](2)).

Table 5-1: Latvia's CND Model [20].

CND Area	Responsible Institutions	Main Tasks
Development of military capabilities and defence strategies	Ministry of Defence, National Armed Forces	Military capability development Defence strategy development Individual willingness to engage in national defence and resist occupation
Closer defence cooperation between private and public sectors	All government bodies	Cross-governmental threat identification and reduction measures Cooperation with NGOs and their involvement in national defence Development of national and local volunteer networks Annual defence training for professionals and experts from various fields Development of the Latvian defence industry and the increase of its role in national defence
Introduction into statehood course for Latvian schools and public awareness-raising	Ministry of Education and Science, Ministry of Defence, other government bodies	National defence curriculum in schools National defence subjects in higher education and science Closer state and society relations
Civil defence and disaster management	Ministry of Interior, local and central government bodies, legal and private entities	Implementation of the seven NATO civil resilience baseline requirements[1] Closer civil-military relations Population readiness to withstand initial stages of disaster or war
Psychological defence	State Chancellery, Ministry of Defence, Ministry of Education and Science, Ministry of Culture, and other responsible authorities	Public resilience to negative campaigns and psychological operations Greater social cohesion Civic engagement in domestic political and social processes Dialogue with religious organisations

[1] NATO's seven baseline requirements are implemented by several ministries and the coordinating role is gradually taken over by the Ministry of Defence.

CND Area	Responsible Institutions	Main Tasks
Strategic communication	State Chancellery, Cross-Sectoral Coordination Centre, and all government bodies	To encourage the population to respond and act in a certain way Government crisis communication Information resilience against the negative portrayal of Latvia
Economic resilience	Ministry of Finance, Ministry of Economics	Provision of essential government services in times of crisis and war Creation of essential commodities reserves at the national level To sustain businesses in times of crisis and war Personal financial security

According to National Security Law, two publicly accessible conceptual documents in national defence are the Concept of National Security and Concept of State Defence. Both these documents must be approved by the Saeima (Parliament of Latvia) not less than once during each convening, i.e., they are reviewed every fourth year. The latest Concept of National Security was adopted in 2019 [11]. The document defines that CND is a foundation of Latvia's national security and national security policy, and names it as one of the priorities for the prevention of military threat. The new Concept of State Defence was adopted in 2020, and the informative report "On Implementation of Comprehensive National Defense System in Latvia" proposed that the Concept includes the fundamental principles of CND as well as the conclusions and proposals of ministries and other institutions regarding the establishment of CND system in Latvia [20]. The Concept of State Defence names four building blocks of Latvia's defence strategy:

- **The National Armed Forces.**
- **Comprehensive Defence.**
- **NATO Collective Defence.**
- **International Cooperation** [37].

According to the Concept of State Defence, the comprehensive defence is the area that focuses primarily on the civilian aspects of the state defence:

> *The goal of comprehensive state defence is to ensure that state institutions, public organizations, and citizens want to defend the state and are ready to provide support to the National Armed Forces and perform vital functions for the existence of society and economy, as well as civil defence activities during the war. The resilience of society is based on psychological resilience to external influences and timely preparation so that in times of crisis and war, all members of society are informed, aware of their responsibilities and desired actions.* [37]

The document outlines several areas related to the CND: continuous operation of the basic functions of the state; societal resilience; protection of the information space; economic sustainability; NGOs; religious organisations; civilian resistance; cybersecurity; and youth education [37].

Further amendments to Latvian legislation are planned to introduce a CND system in Latvia, according to the informative report "On the Progress of the Implementation of a Comprehensive National Defense

System" [25]. To provide society with necessary resources in times of crisis, it was decided to update Regulations of Cabinet on Ministers "On the Provision of Food to the Population in the Event of a State Threat" [4] and "On the Provision of the Population with Basic Industrial Goods in the event of a State Threat" [5]. The National Civil Protection Plan was updated [38]. National Security Law [34] will be amended "to identify critical infrastructure and critical services in the financial sector" and to specify a concept of "situations threatening the country". Mobilisation Law [33] will be amended "to establish exceptions for the recruitment of citizens to active service and the mobilisation of citizens for civil protection formations or implementation of civil protection measures". Several amendments will also be made in the law "On Emergency Situation and State of Exception" [10]: "to ensure the continuity of the functioning of the state and society in the event of a state threat during a declared state of emergency". All amendments are interrelated with the main emphasis on the provision of critical services and continuity of operations during emergency situations.

5.2 THREAT PERCEPTION, NATIONAL OBJECTIVES, AND PRIORITIES

This section describes Latvia's perspective on the security environment, which determines the need for a CND system and the way it is implemented and developed. The main driving forces are the increasing complexity of contemporary threats and Russia's aggressive behaviour in the international arena. However, due to the increasing role of non-military security aspects, at the initial stages, Latvia puts an emphasis on soft aspects of CND such as psychological defence, strategic communication, interinstitutional cooperation, and public preparedness for a crisis.

5.2.1 Threat Perception

The need for a CND system in Latvia is justified with the increasing complexity of threats, which require both military and non-military solutions [19]. The Concept of National Security names several fundamental elements affecting national security environment:

- Hybrid threats that integrate military means and cyber-attacks, operations of foreign intelligence and security services, information and disinformation campaigns, destabilization of society by using inherent contradictions and conflict.
- Climate change.
- Russia's growing military potential, confrontational foreign policy, and attempts to influence internal political processes and public opinion in foreign countries.
- The developments in the Euro-Atlantic space, including Europe and the USA relations, distribution of military expenses among the NATO allies, Brexit, growing populism aimed at the EU disintegration, migration.
- International terrorism [4].

In the context of a CND system development, Russia is mentioned as the main concern in the informative report "On Implementation of Comprehensive National Defense System in Latvia":

> *Russia is currently implementing aggressive foreign policy, strongly challenging security across Europe. Russia has interfered with democratic processes in Europe and the USA, raising real concerns about similar policies being implemented towards Latvia. Nationally and internationally, Latvia has traditionally been heavily influenced by information from the Russian Federation, its political and economic processes, energy policy, and other initiatives.* [20]

However, according to a 2019 study on the willingness of Latvian society to defend the state [2], in the perception of Latvian society, the main threats are related to domestic social, economic, and political issues –

health care system, the standard of living, demographic situation and corruption (Figure 5-1). Russia's policy as a threat is being perceived by 45% of Latvian society in 2019, and in this regard, the polarisation of opinions among two language groups in Latvia can be identified, because 60% of respondents using the Latvian language at home consider Russia's policy as a threat, whereas only 15% of those using the Russian language at home is of opinion that Russia's policy is a threat to the people of Latvia (Figure 5-1). This marks one of the challenges in the introduction of a CND system in Latvia – to achieve a common vision on national security issues among the political elite and society, as well as among the main ethnic group and minorities.

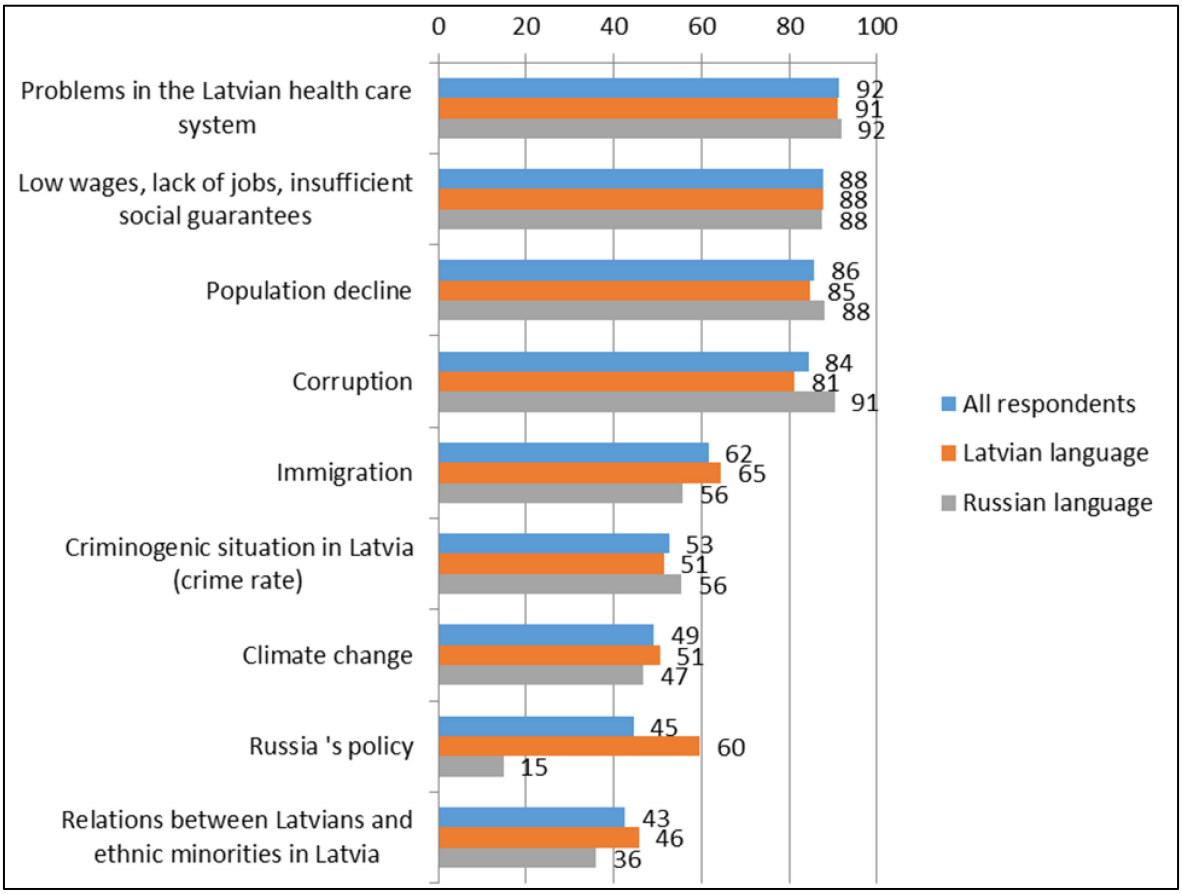

Figure 5-1: Which of the Above, in Your Opinion, Would be Considered the Biggest Threat to the People of Latvia at the Moment? (Number of respondents in the percentage who fully and rather agree) [2].

5.2.2 National Objectives and Priorities

To respond to the changing threat environment and to achieve social cohesion on national security issues, the informative report "On Implementation of Comprehensive National Defense System in Latvia" defines primary tasks to be performed in the short-, medium- and long-term:

- **Development of military capabilities and improvement of defence strategies:** development of the capabilities of the National Armed Forces (NAF), the doctrine of resistance, increasing the role of the National Guard, training of reserve soldiers, improvement of the capabilities of the NAF, planning of dual-use infrastructure.
- **Promotion of public-private partnership in the field of defence:** development of local production, transfer of some NAF support functions to the civil sector, training of public representatives.

- **Teaching the basics of statehood in Latvian schools and educating the public:** introduction of national security curriculum in Latvian schools, seminars for teachers, planning of students' free time.
- **To implement the training specified in regulatory enactments in the field of civil defence.**
- **Psychological defence:** resilience of the population to deliberate and unintentional influences from outside to the information and public environment, ability to maintain rational thinking and decision-making, promotion of critical thinking.
- **Strategic communication:** unified communication of the state aimed to strengthen confidence in the goal of the state's existence, the direction of development, foreign policy choices.
- **The resilience of the economy to crises:** mobilisation of the economy, creation of reserve stocks of economic goods, measures to reduce the consequences of economic crises and protection of the well-being of the population, provision of basic functions for the existence of the economy during the crisis.
- **Strengthening law enforcement and national security institutions:** they are an essential part of a comprehensive national defence system and will be one of the first state institutions to identify and address state threats in the early stages, reducing the potential for escalation [20].

The defined priorities give evidence that Latvia has chosen a balanced approach aimed at step-by-step reducing a variety of internal vulnerabilities that could potentially be exploited by an adversary using a hybrid warfare approach. The Concept of State Defence adopted in 2020 defines two main objectives of the CND: societal resilience in peacetime and the state defence during war. The document outlines detailed tasks of the CND in times of crisis and war:

1) *Public support to the National Armed Forces in ensuring national defence:*
   - *Involvement in the National Armed Forces and organisation of armed resistance;*
   - *Host nation support for Allied forces;*
   - *Implementation of anti-mobility measures;*
   - *Any kind of support to the National Armed Forces, allies (e.g., exchange of information, supply and other activities and events); and*
   - *The resistance movement and the network of supporters, as well as passive resistance (e.g., non-cooperation with the aggressor's armed forces, civil disobedience).*
2) *The capacity of society and the economy to provide critical services and to overcome any shocks, including military conflict:*
   - *The capacity of state power, its effective functioning and continuity;*
   - *Clear tasks and role of each institution and municipality during the war, defining critical personnel and functions;*
   - *The provision of critical services (such as electricity, communications, financial services, food, critical infrastructure, and personnel security) in all circumstances;*
   - *Timely creation and storage of critical service resources and raw material reserves; and*
   - *Timely readiness to respond to crisis and war situations at different levels of society, including individual civic readiness* [37].

5.3 NATIONAL AND INTERNATIONAL INTEROPERABILITY

This section describes how Latvia builds and maintains resilience at a national level by coordination and integration of resources and efforts of all major governing bodies, army, and other force structures and facilitate the practical implementation of collective defence principles.

5.3.1 CND System Implementation

To implement CND, the Ministerial Working Group was created in 2019. On April 2, 2019, the informative report "On the Comprehensive National Defense Coordination Working Group" [23] was considered at the sitting of the Cabinet of Ministers, and the respective Order of the Cabinet of Ministers "On the Working Group" [6] was adopted on April 4, 2019. The chief of the Ministerial Working Group was A. Pabriks, Deputy Prime Minister and Minister of Defence, because "the Ministry of Defense is the responsible public administration institution that coordinates the implementation of a comprehensive national defence system, providing support to all sectors in identifying threats and challenges and formulating solutions" (Figure 5-2) [23]. The Working Group provides political level monitoring and coordination of the implementation of CND and is modelled by the example of Nordic countries and Estonia.

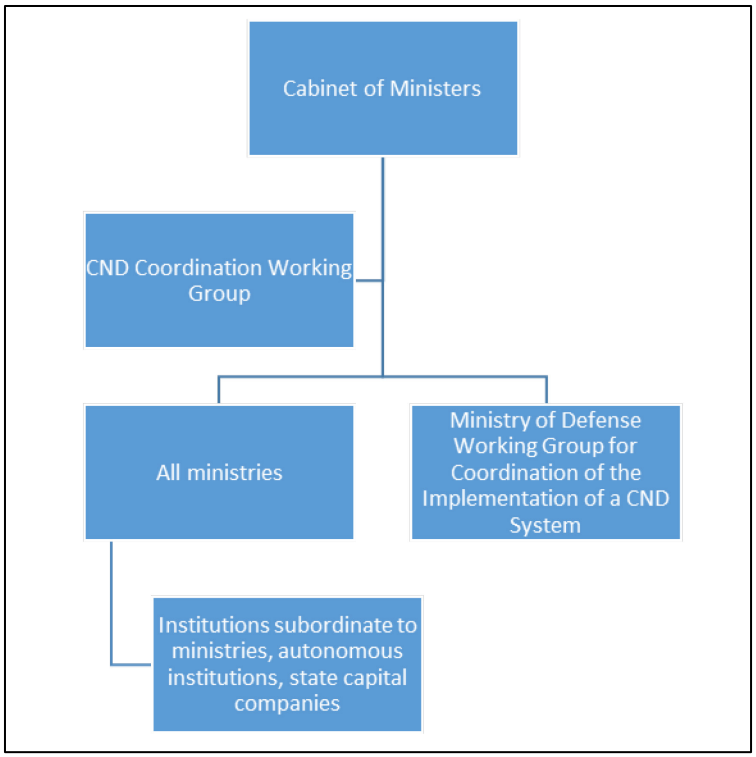

Figure 5-2: The Hierarchical Role of the Ministerial Working Group [23].

In 2019, the working group was convened for three meetings, and it is admitted in the Informative Report "On the Progress of the Implementation of a Comprehensive National Defense System": "The established co-operation between the ministries within the framework of the Ministerial Working Group has enhanced the understanding of the process of implementation of CND among the ministries" [26]. A CND working group of state secretaries chaired by the state secretary of the Ministry of Defense has also been established in Latvia. Ministries can also set up their own internal working groups.

Thus, for the time being in Latvia, new structures related to the CND system are not being created, but the emphasis is being put on increasing the effectiveness of cooperation among existing structures, and the improvement of the existing legal framework and applying the defined principles in the practice. However, at a political level, there are ideas that further development of the CND system eventually will require new structures. For example, in the opinion of R. Bergmanis, the Chairman of Comprehensive National Defence Subcommittee of the Defence, Internal Affairs and Corruption Prevention Committee of the Saeima and former Minister of Defence: "Probably one of the tools with which we could very well protect ourselves

would be the crisis management center that exists in many countries around the world. Such a center should be open 24 hours a day, seven days a week, and should be prepared to respond to any kind of crisis – natural disasters, epidemics, accidents, or political crises – so that the country is prepared to withstand such dramatic shocks" [8].

5.3.2 Crisis Management Organisation

Crisis management organisation is defined by the National Security Law. The law provides that "in the case of a threat to national security, the Crisis Management Council shall coordinate civilian-military cooperation and the operational measures of State administration authorities in overcoming the threat to national security" [34] (Section 23^{1} (1)). The Crisis Management Council is chaired by the Prime Minister and it is formed by the Ministers of nine ministries: Defence; Foreign Affairs; Economics; Finance; the Interior; Justice; Health; Transport; Environmental Protection and Regional Development [34] (Section $23.^{2}$ (1), (2)). The main functions of the Crisis Management Council are to co-ordinate "to coordinate "the operational management of overcoming the threat to national security", "the development of plans for the prevention of threat to national security of State administration authorities", "in the case of a threat to national security…a unified and timely implementation of political decisions in State administration authorities" [34] (Section $23.^{3}$). The detailed outline of the functions is defined in the By-law of the Crisis Management Council [12]. The meetings of the Crisis Management Council take place not less than once in six months and the work of the Secretariat is provided by the Ministry of Interior [12].

The COVID-19 case provides an example of how the crisis management system operates in Latvia. The Crisis Management Council held five meetings during February and March 2020 on the current situation with the COVID-19 pandemic [48]. The emergency was declared on March 12, 2020 [7], and the Group for Coordination of Interinstitutional Activities was established on March 16, 2020, to coordinate the activities of the institutions involved in containing the spread of COVID-19 [39]. A. Pabriks, Deputy Prime Minister and Minister of Defence admitted that the COVID-19 pandemic affirmed the need for the CND system: "The global crisis caused by COVID-19 has highlighted several challenges and provided an opportunity to conclude critical services and the way forward for various crises. It is essential for us to provide critical services in various types of potential crises, so we need to set a minimum basket of critical services and make it an obligation to provide it to citizens in any situation" [27]. Despite the organisational problems highlighted by the COVID-19 pandemic, Latvia experienced relatively low numbers of infected and dead, and the magazine "Foreign Policy" even named Latvia "the coronavirus pandemic's success story", which according to the report was determined by rapid reaction and trust to experts [41].

5.3.3 Crisis Exercises "Kristaps"

To improve the capacity of senior state officials to participate in national defence, Latvia holds yearly strategic level decision-making crisis management exercises "Kristaps", involving all ministries, the President of Latvia, members of parliament, key industry leaders, NGOs, etc. In 2019 the training was aimed at "the improvement of practical and theoretical skills in state threat management planning, decision-making and implementation of planned measures" [24]. The financial sector also participated in the training, to improve the resilience towards various crisis scenarios [47]. In 2018 the crisis training was part of military training, "Namejs 2018". The senior state officials improved their skills to overcome a conventional threat [21]. In 2017 and 2016 the government trained to overcome hybrid threats [18], [17]. In 2015 government crisis training was integrated with NATO training "Arrcade Fusion 2015" and the Baltic States host nation support planning exercises "Baltic Host 2015", which all together improved the necessary skills to operate in the current security environment at the national and international level [16]. This way Latvia gradually increases the knowledge and skills of higher state officials to operate in crisis situations in a coordinated and integrated manner, which is a practical implementation of the whole-of-government principle.

5.3.4 Interdepartmental Cooperation

Within the framework of civil-military cooperation, Latvian National Armed Forces (NAF) cooperates with state, local government, and private institutions to overcome national threats. Main organisations supported by the NAF are:

- **Latvian State Security Service** – in counter-terrorism measures, as well as in measures for the prevention or management of terrorist threats.
- **The civil defence system** – in preventive and response measures, urgent measures for elimination of the consequences of events that have caused an emergency situation, as well as in rescue and search works.
- **Latvian State Police** – in ensuring public order and security.
- **The State Border Guard** – in ensuring the inviolability of the state border.
- **Latvian Cadet Force** – in the implementation of the youth interest education program.
- **State security institutions** – in the performance of national security measures [31].

During the COVID-19 pandemic, the NAF supported the State Border Guard, which was positively evaluated by its chief, General G. Pujats: "It is positive that we have developed operational cooperation at this level, and local national guards (*the voluntary National Guard is an integral part of the NAF*) have also had a much better opportunity to get to know the local area and to develop cooperation on a daily basis for various scenarios in the future. As a neighbour, Latvia has been a good example to neighbouring countries in terms of integrity and co-operation between various services, including between the National Armed Forces and the State Border Guard" [44]. The National Guard also cooperated with the State Policy to prevent COVID-19 prevalence in Latvia. The Commander of the 1st Riga Brigade of the National Guard, Lieutenant Colonel A. Krjukovs notes that the co-operation model with the State Police is being developed on a gradual basis through joint training and support in daily tasks such as the search of missing people [45]. The Concept of State Defence determines that "in the event of a military attack, the State Border Guard and the Defense Department of the Bank of Latvia join the NAF, thus strengthening the national defense capabilities" [37]. Closer integration and interoperability of these forces can be achieved by implementing "common NATO standards and by providing basic military training for personnel." [37]

5.3.5 International Interoperability

NATO's enhanced forward presence battlegroup led by Canada was fully deployed in Latvia in 2017. Working closely with the Land Forces Mechanized Infantry Brigade, NATO eFP battle group "will improve interoperability with regional allies and be able to respond to the changing security environment" [29]. The establishment of Headquarters Multinational Division North in Latvia in 2019 by Denmark, Estonia, and Latvia is another significant step to increase international interoperability because it "is tasked with defence planning, military training, planning, and coordination of common projects. It will promote the compatibility of forces from participating countries and their interoperability in the scope of common defence initiatives" [22]. International interoperability is also strengthened by regional cooperation, which is closest to the neighbouring Baltic States and takes place at various levels, including joint military training [30].

Under the conditions of military invasion, within the framework of NATO, Latvia provides host nation support to Allied forces, as well as NATO and European Union organisations located in the territory of Latvia [32]. In 2017 Latvia signed the agreement on host nation support to NATO's Very High Readiness Joint Task Force, which provides rapid arrival of a military unit and serves as a deterrent for potential aggressor [9]. During NATO's deployment exercise Ramstein Dust-II 2017, the host nation support provided by Latvia was positively evaluated by the exercise director, German Air Force Colonel K. Nolte, who named it as an example of "Alliance cohesion and interoperability" [36]. Latvia has made many amendments to its

laws to facilitate the presence of Allied forces. An important area is military mobility, which faces huge bureaucracy [40]. For example, in 2016 Latvia adopted new regulations to facilitate the entry of NATO warships into Latvian waters [46]. To ensure the rapid deployment of Allied forces within NATO and the EU, the Ministry of Defence plans to achieve the construction of Rail Baltica railway branch to Ādaži military base [43]. For the host nation support, it is also important to develop Liepāja port and Lielvārde airport, as well as to adjust the roads and bridges being repaired to the parameters of military mobility agreed between NATO and EU members [37].

5.4 CHALLENGES OF IMPLEMENTATION

CND aims to involve the whole of society in state defence; therefore, it raises issues related to state and society relations and social cohesion. The analysis of the vulnerabilities of Latvian society amid Russia's annexation of Crimea and following war in south-eastern Ukraine revealed two significant cleavages in Latvian society related to the ethnic structure and estrangement between society and the state [1]. These issues are also relevant in the context of the development of the CND system. The study of the willingness of Latvian society to defend a country in the context of CND gives evidence that it is positively affected by such factors as knowledge of CND and crisis management; historical examples of heroism; belief that Latvian public administration institutions operate for the common good; and effective communication with public administration institutions and local governments [3]. Nevertheless, the majority of a population in Latvia distrust parliament and government, because only around one third admits trusting these institutions, while president and municipalities are trusted by half of the population [3] (p.13). The study also discovered the more pronounced alienation of Latvia's ethnic minorities from the state, which is one of the reasons that decrease the overall indicators of the willingness of Latvian society to defend a country [3]. In the context of CND system implementation, it poses a challenge to achieve a common vision on security issues in both language groups.

Latvia also experiences constant pressure from Russia in the media environment, and the implementation of the CND system is no exception. The internet portals owned by international information agency Russia Today LV.sputniknews.ru and LV.baltnews.com promoted several narratives aimed to discredit CND in Latvia:

- The state is unable to ensure the security of the population [13].
- CND is being implemented against the will of the population [15].
- Russia's threat is exaggerated [14].
- The people of Latvia are not ready to defend the country [14].
- Latvia cannot defend itself without NATO [15].
- Latvia makes itself a priority target in the event of a global military conflict [15] and others.

Such activities in the information space aim to reduce public support to CND system implementation by ridiculing it and constructing contradictory narratives that Russia is not a military threat, but at the same time, Latvia will be a target in case of military conflict. This gives evidence that concerning CND system implementation the Latvian government and defence sector in particular should focus not only on change management but also has to overcome destructive trends in the information environment.

5.5 FUTURE DEVELOPMENTS AND ONGOING DISCUSSIONS

At the end of 2019, the Minister of Defence A. Pabriks informed society about the progress of the implementation of CND in Latvia [42]. The Minister outlined the intention to implement CND until 2024, and he mentioned some of the most important things that had already been done:

- Several exercises for law enforcement and state institutions' employees to improve theoretical and practical skills necessary for overcoming danger to the state;
- Crisis training for commercial organisations, NGOs and municipalities;
- Educating and preparing the public for potential crises;
- Implementation of state defence curriculum of school programs, which will be mandatory from 2024;
- Launching a news portal dedicated to the defence issues;
- Cooperation with Latvian defence industry; and
- Unscheduled combat readiness tests.

On June 3, 2020, the Latvian Ministry of Defence launched an informative brochure "What to Do in Case of Crisis" [28]. The brochure is an integral part of the campaign "72 hours" which is aimed at preparing the public to withstand the first three days of any crisis.

For the time being, the CND system in Latvia primarily is a way of thinking because current activities are aimed at informing and educating the representatives of the responsible and involved institutions, as well as society in general. So far, the focus has been on the more effective use of existing structures and resources. The three pillars of the CND mindset are:

1) Resistance – in case of military attack Latvia will resist;
2) Responsibility – national security is a responsibility of every member of Latvian society; and
3) Cooperation – force structures, public administration institutions, municipalities, NGOs, commercial organisations, and individual members of society cooperate to protect Latvian statehood.

5.6 REFERENCES

[1] Berzina, I. (Ed.). (2016), The Possibility of Societal Destabilization in Latvia: Potential National Security Threats. National Defence Academy of Latvia, Center for Security and Strategic Research, https://www.academia.edu/37621540/The_Possibility_of_Societal_Destabilization_in_Latvia_Potential_National_Security_Threats, Accessed 2 June 2020.

[2] Berzina, I., and Zupa, U. (2020), Latvijas sabiedrības griba aizstāvēt valsti: veicinošie un kavējošie faktori [The Will of Latvian Society to Defend the State: Facilitating and Disincentive Factors]. National Defence Academy of Latvia, Center for Security and Strategic Research, https://www.naa.mil.lv/sites/naa/files/document/DSPC_GribaAizstavetValsti_0.pdf, Accessed 28 May 2020.

[3] Berzina, I., and Zupa, U. (2020), Latvijas sabiedrības griba aizstāvēt valsti: veicinošie un kavējošie faktori [The Will of Latvian Society to Defend the State: Facilitating and Disincentive Factors]. National Defence Academy of Latvia, Center for Security and Strategic Research, https://www.naa.mil.lv/sites/naa/files/document/DSPC_GribaAizstavetValsti_0.pdf, Accessed 28 May 2020.

[4] Cabinet of Ministers (2007) Noteikumi Nr. 585 "Noteikumi par iedzīvotāju nodrošināšanu ar pārtiku valsts apdraudējuma gadījumā" [Regulation no. 585 "Regulation on Provision of Food to the Population in Case of State Threat"], https://likumi.lv/ta/id/162510-noteikumi-par-iedzivotaju-nodrosinasanu-ar-partiku-valsts-apdraudejuma-gadijuma, Accessed 25 May 2020.

[5] Cabinet of Ministers (2015) Noteikumi Nr. 755 "Noteikumi par iedzīvotāju nodrošināšanu ar pirmās nepieciešamības rūpniecības precēm valsts apdraudējuma gadījumā" [Regulation no. 755 "Regulation on Providing the Population with Essential Industrial Goods in the Event of a State Threat"], https://likumi.lv/ta/id/278820-noteikumi-par-iedzivotaju-nodrosinasanu-ar-pirmas-nepieciesamibas-rupniecibas-precem-valsts-apdraudejuma-gadijuma, Accessed 25 May 2020.

[6] Cabinet of Ministers (2019), Rīkojums nr. 155 „Par darba grupu [Order no. 155 „On the Working Group"], https://likumi.lv/ta/id/306040-par-darba-grupu, Accessed 18 May 2020.

[7] Cabinet of Ministers (2020), Order no. 103 "Regarding Declaration of the Emergency Situation", https://likumi.lv/ta/en/en/id/313191, Accessed 1 Jun 2020.

[8] Krautmanis, M. (2020), Raimonds Bergmanis: Bez kavēšanās jāizveido krīzes centrs [Raimonds Bergmanis: A crisis center must be established without delay], NRA.lv, April 15, https://nra.lv/latvija/311125-raimonds-bergmanis-bez-kavesanas-jaizveido-krizes-centrs.htm, Accessed 2 Jun 2020.

[9] Latvian Public Broadcasting (2017), Latvia prepares NATO crisis response agreement, https://eng.lsm.lv/article/society/defense/latvia-prepares-nato-crisis-response-agreement.a221738/, Accessed 12 August 2020.

[10] Latvijas Vēstnesis (2013), On Emergency Situation and State of Exception, https://likumi.lv/ta/en/en/id/255713, Accessed 25 May 2020.

[11] Likumi: Legal Acts of the Republic of Latvia (2019). On Approval of the National Security Concept , https://likumi.lv/ta/en/en/id/309647, Accessed 21 May 2020.

[12] Likumi: Legal Acts of the Republic of Latvia, By-law of the Crisis Management Council. (2011), https://likumi.lv/ta/en/en/id/224553, Accessed 1 Jun 2020.

[13] LV.baltnews.com (2019), "Защити себя сам". Как Минобороны Латвии собирается избавить граждан от эгоизма ["Protect yourself." How the Ministry of Defense of Latvia is going to save citizens from selfishness], April 30, https://lv.baltnews.com/riga_news/20190430/1022977141/zashchiti-sebya-sam-kak-minoborony-latvia-sobiraetsya-izbavit-grazhdan-ot-ehgoizma.html, Accessed 2 June 2020.

[14] LV.baltnews.com (2019), Армии нет, но вы держитесь: новая латвийская памятка о "вторжении" [There is no army, but you hold on: a new Latvian memo on the "invasion"], November 14, https://lv.baltnews.com/nato/20191114/1023501655/Armii-net-no-vy-derzhites-novaya-latviyskaya-pamyatka-o-vtorzhenii.html, Accessed 2 June 2020.

[15] LV.sputniknews.ru (2019), Хватит нас пугать: латвийцы просят Минобороны прекратить говорить о вторжении [Stop scaring us: Latvians ask the Ministry of Defense to stop talking about the invasion], November 11, https://lv.sputniknews.ru/Latvia/20191111/12742054/Khvatit-nas-pugat-latviytsy-prosyat-Minoborony-prekratit-govorit-o-vtorzhenii.html, Accessed 2 June 2020.

[16] Ministry of Defence (2015), Mācībās "Kristaps 2015" pārbauda Ministru kabineta spējas darboties pašreizējā drošības vidē [In the exercise "Kristaps 2015" examines the ability of the Cabinet of Ministers to operate in the current security environment], November 10, https://mk.gov.lv/lv/aktualitates/macibas-kristaps-2015-parbauda-ministru-kabineta-spejas-darboties-pasreizeja-drosibas, Accessed 12 August 2020.

[17] Ministry of Defence (2016), Mācībās "Kristaps 2016" pilnveido valdības praktiskās iemaņas pārvarēt hibrīdapdraudējumu [In the training "Kristaps 2016" improves the government's practical skills to overcome the hybrid threat], October 17, https://www.mod.gov.lv/lv/zinas/macibas-kristaps-2016-pilnveido-valdibas-praktiskas-iemanas-parvaret-hibridapdraudejumu, Accessed 12 August 2020.

[18] Ministry of Defence (2017), Mācībās "Kristaps 2017" pilnveido valdības praktiskās iemaņas pārvarēt hibrīdapdraudējumu [In the training "Kristaps 2017" improves the government's practical skills to overcome the hybrid threat], October 16, https://www.mod.gov.lv/lv/zinas/macibas-kristaps-2017-pilnveido-valdibas-praktiskas-iemanas-parvaret-hibridapdraudejumu, Accessed 12 August 2020.

[19] Ministry of Defence (2018) Informatīvais ziņojums "Par visaptverošas valsts aizsardzības sistēmas ieviešanu Latvijā" [Informative Report "On Implementation of Comprehensive National Defense System in Latvia"], http://tap.mk.gov.lv/lv/mk/tap/?pid=40462120&mode=mk&date=2019-01-08, Accessed 11 March 2020.

[20] Ministry of Defence (2018), Informatīvais ziņojums "Par visaptverošas valsts aizsardzības sistēmas ieviešanu Latvijā" [Informative Report "On Implementation of Comprehensive National Defense System in Latvia"], http://tap.mk.gov.lv/lv/mk/tap/?pid=40462120&mode=mk&date=2019-01-08, Accessed 11 March 2020.

[21] Ministry of Defence (2018), Mācībās "Kristaps 2018" pilnveido valsts augstāko amatpersonu praktiskās iemaņas pārvarēt konvenciālu iebrukumu [Kristaps 2018 improves practical skills of senior state officials to overcome a conventional invasion], August 21, https://www.mod.gov.lv/lv/zinas/macibas-kristaps-2018-pilnveido-valsts-augstako-amatpersonu-praktiskas-iemanas-parvaret, Accessed 12 August 2020.

[22] Ministry of Defence (2019), Inauguration of Headquarters Multinational Division North in Camp Ādaži, https://www.mod.gov.lv/en/news/inauguration-headquarters-multinational-division-north-camp-adazi, Accessed 13 August 2020.

[23] Ministry of Defence (2019), Informatīvais ziņojums „Par visaptverošas valsts aizsardzības jautājumu koordinācijas darba grupu"[Informative Report „On the Comprehensive National Defense Coordination Working Group"], http://tap.mk.gov.lv/lv/mk/tap/?pid=40470707&mode=mk&date=2019-04-02, Accessed 18 May 2020.

[24] Ministry of Defence (2019), Mācībās "Kristaps 2019" pilnveido valsts augstāko amatpersonu praktiskās iemaņas pārvarēt valsts apdraudējuma situācijas [In the training "Kristaps 2019" improves the practical skills of the highest state officials to overcome state threat situations], October 14, https://www.mil.lv/lv/zinas/macibas-kristaps-2019-pilnveido-valsts-augstako-amatpersonu-praktiskas-iemanas-parvaret, Accessed 12 August 2020.

[25] Ministry of Defence (2020) Informatīvais ziņojums "Par visaptverošas valsts aizsardzības sistēmas ieviešanas progresu" [Informative Report "On the progress of the implementation of a comprehensive national defense system"], http://tap.mk.gov.lv/lv/mk/tap/?pid=40484513, Accessed 25 May 2020.

[26] Ministry of Defence (2020), Informatīvais ziņojums "Par visaptverošas valsts aizsardzības sistēmas ieviešanas progresu" [Informative Report "On the progress of the implementation of a comprehensive national defense system"], http://tap.mk.gov.lv/lv/mk/tap/?pid=40484513, Accessed 25 May 2020.

[27] Ministry of Defence (2020), Pabriks: COVID-19 krīze apliecina nepieciešamību pēc visaptverošas valsts aizsardzības sistēmas [Pabriks: The COVID-19 crisis confirms the need for a comprehensive national defense system], March 17, https://www.mod.gov.lv/lv/zinas/pabriks-covid-19-krize-apliecina-nepieciesamibu-pec-visaptverosas-valsts-aizsardzibas, Accessed 2 Jun 2020.

[28] Ministry of Defence (2020). Brochure "What to do in case of crisis", Available at https://www.sargs.lv/lv/brochure-what-to-do-in-case-of-crisis, Accessed 4 June 2020.

[29] Ministry of Defence (n.d.), NATO paplašinātās klātbūtnes kaujas grupa [NATO eFP battlegroup], https://www.mod.gov.lv/index.php/lv/nato/nato-militaras-spejas/nato-paplasinatas-klatbutnes-kaujas-grupa, Accessed 13 August 2020.

[30] Ministry of Defence (n.d.), Regional cooperation, https://www.mod.gov.lv/en/nozares-politika/international-and-regional-cooperation/regional-cooperation, Accessed 12 August 2020.

[31] Ministry of Defence (n.d.), Sadarbība [Cooperation], Available at https://www.mil.lv/lv/par-mums/par-nbs/sadarbiba, Accessed 12 August 2020.

[32] Ministry of Defence (n.d.), Uzņemošās valsts atbalsts [Host Nation Support], https://www.mil.lv/lv/par-mums/par-nbs/sadarbiba/uznemosas-valsts-atbalsts, Accessed 12 August 2020.

[33] Mobilisation Law (2002), https://likumi.lv/ta/en/en/id/63407, Accessed 25 May 2020.

[34] National Security Law (2000), Section 2, https://likumi.lv/ta/en/en/id/14011, Accessed 19 May 2020.

[35] National Security Law (2000), Section 23.5, https://likumi.lv/ta/en/en/id/14011, Accessed 19 May 2020.

[36] NATO (2017), "Latvia showcases host nation support during NATO exercise", https://ac.nato.int/archive/2017/latvia-showcases-host-nation-support-during-nato-exercise–2, Accessed 12 August 2020.

[37] Par Valsts aizsardzības koncepcija apstiprināšanu [On Approval of the Concept of State Defence] (2020), https://likumi.lv/ta/id/317591-par-valsts-aizsardzibas-koncepcijas-apstiprinasanu, Accessed 10 November 2020.

[38] Par Valsts civilās aizsardzības plānu [On National Civil Protection Plan] (2020), https://likumi.lv/ta/id/317006-par-valsts-civilas-aizsardzibas-planu, Accessed 10 November 2020.

[39] Prime Minister (2020), Order no. 2020/1.2.1.-60 "Regarding the Group for Coordination of Interinstitutional Activities", https://likumi.lv/ta/en/en/id/313245, Accessed 1 Jun 2020.

[40] Rakstiņš, V. (2018), Militārā mobilitāte – spēja ātri pārvietot spēkus [Military mobility – the ability to move forces quickly], https://www.sargs.lv/lv/nozares-politika/2018-06-29/militara-mobilitate-speja-atri-parvietot-spekus, Accessed 13 August 2020.

[41] Sander, F.G. (2020), Facing Pandemic, Latvia Follows the Lead of Its Experts. *FP*, May 13, https://foreignpolicy.com/2020/05/13/coronavirus-pandemic-latvia-follows-lead-medical-experts-science/, Accessed 1 Jun 2020.

[42] Sargs.lv (2019), Pabriks: visaptverošas valsts aizsardzības sistēmu plānots ieviest līdz 2024. Gadam [Pabriks: A comprehensive national defense system is planned to be in place by 2024], https://www.sargs.lv/lv/nozares-politika/2019-12-12/pabriks-visaptverosas-valsts-aizsardzibas-sistemu-planots-ieviest-lidz, Accessed 18 May 2020.

[43] Sargs.lv (2020), Aizsardzības ministrija plāno panākt "Rail Baltic" atzara būvniecību uz Ādažu militāro bāzi [The Ministry of Defense plans to achieve the construction of the Rail Baltica branch on the Ādaži military base], https://www.sargs.lv/lv/nbs/2020-06-25/aizsardzibas-ministrija-plano-panakt-rail-baltic-atzara-buvniecibu-uz-adazu-militaro, Accessed 12 August 2020.

[44] Sargs.lv (2020), Valsts robežsardzes priekšnieks: Latvija starpresoru sadarbības jomā kaimiņvalstīm ir labs piemērs [Chief of the State Border Guard: Latvia is a good example for neighboring countries in the field of inter-ministerial co-operation], July 14, https://www.sargs.lv/lv/nbs/2020-07-14/valsts-robezsardzes-prieksnieks-latvija-starpresoru-sadarbibas-joma-kaiminvalstim-ir, Accessed 12 August 2020.

[45] Sargs.lv (2020), Zemessardzes 1. Rīgas brigādes komandieris: krīze stiprinājusi dienestu savstarpējo sadarbību [Commander of the 1st Riga Brigade of the National Guard: the crisis has strengthened interdepartmental cooperation], May 21, https://www.sargs.lv/lv/nbs/2020-05-21/zemessardzes-1-rigas-brigades-komandieris-krize-stiprinajusi-dienestu-savstarpejo, Accessed 12 August 2020.

[46] Sargs.lv. (2016), Atvieglos NATO karakuģu ienākšanu Latvijas ūdeņos [The entry of NATO warships into Latvian waters will be facilitated], https://www.sargs.lv/lv/nozares-politika/2016-02-23/atvieglos-nato-karakugu-ienaksanu-latvijas-udenos, Accessed 13 August 2020.

[47] The Baltic Times (2019), Defense Ministry and banks play out crisis scenario in an exercise, August 8, https://www.baltictimes.com/defense_ministry_and_banks_play_out_crisis_scenario_in_an_exercise/, Accessed 12 August 2020.

[48] The State Fire and Rescue Service (2020), Krīzes vadības padomes 2020. gada sēdes [Crisis Management Council meetings in 2020], https://vugd.gov.lv/lat/par_vugd/darbibas_sferas/krizes_vadibas_padomes_2020_gada_sedes/, Accessed 1 Jun 2020.

Chapter 6 – NORWEGIAN CASE STUDY

Monica Endregard
Norwegian Defence Research Establishment
NORWAY

6.1 INTRODUCTION

The purpose of this case study is to describe Norway's approach to securing the nation state and the society against external and internal threats and hazards. Threats range from natural and manmade disasters through hybrid threats to use of military force. Being a small country with limited resources, a fundamental principle for emergency prevention, preparedness and response in Norway is to make efficient use of all available resources. This entails extensive cooperation between civil and military entities as well as private actors.

The emphasis of this NATO study is on civil-military cooperation within the framework of a comprehensive national defence concept. Comprehensive defence is understood as situations involving the military either in lead or support role. Norwegian authorities refer to this as civil-military cooperation in the framework of *the Norwegian total defence concept*.

The introductory section presents a brief background in Norway, key definitions, the governing principles for emergency preparedness and crisis management and finally the responsibilities and organisation of central crisis management. The second section focusses on the Norwegian threat perception, national objectives, and priorities. The third section presents a short resume of the evolution of the total defence concept in Norway and the total defence today. The fourth section emphasises national and international interoperability in crises management within the framework of the total defence concept. The fifth section of this Norwegian case study sums up some key challenges, and the final section presents plans for future developments and ongoing discussions related to total defence in Norway.

6.1.1 Background and Norwegian Governing Principles

The Kingdom of Norway is a parliamentarian, democratic, unitary, and constitutional monarchy with a population of 5.4 million (2020) [27]. The King of Norway is the head of state and the Prime Minister is the head of Government. The power is divided between three branches: a legislative branch also responsible for appropriations, the Storting (the Parliament); an executive branch, the Government (Cabinet), and a judicial branch, the courts. The Constitution of 17 May 1814 serves as the country's supreme legal document. The Prime Minister and ministers constitute the Government. As of 24 January 2020, there are 19 ministers and 15 ministries [9]. Each minister has constitutional responsibility within his/her area.

Norway is divided into eleven first-level administrative counties (fylker – singular fylke) (per 1 January 2020). The counties are administered through directly elected county assemblies headed by a Chairman of the county (fylkesordfører). Additionally, the Government is represented in every county by a County Governor (fylkesmann) to implement the Parliament's and Government's decisions. The King in Council appoints a County Governor, who is responsible for the administration of national affairs at the county level. The counties are sub-divided into 356 second-level municipalities (kommuner – singular kommune), which in turn are administered by directly elected municipal councils, headed by a mayor and a small executive cabinet. The capital, Oslo, is both a county and a municipality.

The Government has the overall executive responsibility for state security, societal security and emergency prevention, preparedness planning and crisis management:

> *The overall objective for Norwegian security and defence policy is to protect and defend Norwegian sovereignty, territorial integrity, democratic institutions and freedom of action against political, military and other pressure* (Ref. [13], [14], p, 4, Prop. 14 S (2020 – 2021)).

A challenge or threat to the state's security could spur various governmental actions, often a combination of political, diplomatic, economic, or military means. The top national political level handles matter of state security. The Armed Forces' key task is to contribute to maintaining state security.

Societal security (or public security) is defined as:

> *Society's ability to protect itself against, and manage, incidents that threaten fundamental values and functions and that put lives and health in danger. Such incidents may be caused by nature, by technical or human error, or by intentional acts.* (Ref. [15], Executive Summary. Page 8).

Mainly, the work on societal security is assigned to the individual ministry, its subordinate governmental agencies, and the municipalities. The Ministry of Justice and Public Security has a general coordinating role on the civil side for public security, civil protection, and emergency preparedness, as well as for Information and Communication Technology (ICT) security [23]. The Directorate for Civil Protection supports the ministry in its general coordinating societal security role [26]. The National Security Service has a corresponding role in the field of ICT security. The County Governor has a regional coordinating role for civil protection [1].

Norway bases her societal security, emergency preparedness and crisis management on four fundamental principles: responsibility, similarity, proximity, and cooperation (Ref. [15], p. 9):

- Principle on responsibility: that the organisation responsible for an area on a day-to-day basis is also responsible for the necessary emergency preparedness preparations and for managing extraordinary incidents in that area.
- Principle of similarity: that the organisation one operates with during a crisis should be as similar as possible to the day-to-day organisation.
- Principle of proximity: that crises should be handled organisationally at the lowest possible level.
- Principle of collaboration: that authorities, enterprises, or agencies have an independent responsibility to ensure the best possible cooperation with relevant parties and enterprises on work related to prevention, emergency preparedness and crisis management.

In addition to these fundamental principles, Norway emphasises civil-military cooperation to manage severe crises. After the Second World War Norway established the "total defence concept" to ensure the full mobilisation of the society's limited resources to defend the nation against an existential threat. In 2004, the authorities modernised and broadened the total defence concept (Ref. [10], p. 10):

> *The modernised total defence concept encompasses mutual support and cooperation between the Norwegian Armed Forces and civil society in connection with contingency planning, crisis management and consequence management across the entire crisis spectrum – from peace via security policy crises to armed conflict.*

Section 6.3 will explain the total defence concept, describe roles and responsibilities of some of the key actors and refer to relevant doctrines and legislation.

6.1.2 Organisation of Central Crisis Management

The *Instructions for the ministries' work with civil protection and emergency preparedness* describe the framework for central crisis management **Error! Reference source not found.**. The Government has political responsibility for emergency preparedness and crisis management. Each minister has constitutional responsibility within his/her area, also during a crisis.

The Governmental Security Council (Regjeringens sikkerhetsråd) is the primary body for discussing security issues. The permanent members are the Prime Minister, the Minister of Foreign Affairs, the Minister of Defence, the Minister of Justice and Public Security and the Minister of Finance.

In accordance with the responsibility principle, the ministry responsible for a sector is also responsible for emergency preparedness planning and action in a crisis. The Ministry of Justice and Public Security has a particular responsibility for coordinating the administration of work on safety, security, and emergency planning within the civil sector [23]. This includes responsibility for developing new national guidelines, making principal decisions regarding the Norwegian civil preparedness system and administrative responsibility for the Search and Rescue Service.

The Crisis Council (Kriserådet) is the principal administrative coordinating body at the ministries level. The five permanent members are the Secretary to the Government from the Office of the Prime Minister, the Deputy Secretary General from the Ministry of Foreign Affairs and the Secretary Generals from the Ministry of Justice and Public Security, Ministry of Defence and the Ministry of Health and Care Services. The Crisis Council is expanded to include other ministries when needed. In addition, representatives for subordinate enterprises and expert groups participate if required. All ministries can take the initiative to summon the Council.

The Crisis Council is authorised by the Government to determine which ministry shall be the lead ministry during management of an incident. The lead ministry coordinates the management of the crisis at the central level. The Ministry of Justice and Public Security is the permanent lead ministry for national civil crises unless otherwise decided. The designation of a lead ministry does not affect constitutional responsibilities. All ministries retain the responsibility and decision-making authority for their respective areas.

The Crisis Support Unit (Krisestøtteenheten) shall provide support to the lead ministry and the Crisis Council. The Crisis Support Unit is the secretariat for the Crisis Council. It administratively under the Department of Public Security in the Ministry of Justice and Public Security and a part of the Civil Situation Centre, the permanent point of contact for information to and from the Ministry of Justice and Public Security in the event of extraordinary incidents and crises. The Crisis Support Unit contributes expertise, advice and support for analyses, the preparation and communication of overall situation reports and establishing a joint understanding of the situation as a basis for strategic decisions. The support includes infrastructure (including technical solutions), premises and personnel.

6.2 THREAT PERCEPTION, NATIONAL OBJECTIVES AND PRIORITIES

This section summarises the Norwegian threat perception based on national threat and risk assessments as presented in official documents by the Government and security agencies. Finally, the section presents national objectives and priorities for civil-military cooperation to safeguard state security and societal security.

6.2.1 Threat Perception

This sub-section gives a brief overview of Norwegian authorities' threat perspective and views on Norwegian security and safety challenges from both external and internal threats and hazards, as conveyed in official documents and reports.

In the Long-Term Defence Plan the Government states, "Norway and our allies face a new and deteriorating security situation" (Ref. [13], p.2). The threat and risk picture is diverse, composed of terrorist and cyber-attacks, extreme weather events such as flooding and wildfires, and a security policy situation that could develop into crises. Four key Norwegian agencies publish threat and risk assessments each year to inform politicians, official stakeholders, and the public.

The Norwegian Intelligence Service, subordinate to The Norwegian Chief of Defence, is Norway's foreign intelligence service. Its main missions are

1) To warn of external threats to Norway and Norwegian high priority interests;
2) To support the Norwegian Armed Forces and Norway's defence allies; and
3) To provide information to political and administrative decision-makers about topics of significance to Norwegian foreign, security and defence policy.

The annual report Focus 2020 presents the Service's assessment of the current situation and expected developments of particular Norwegian relevance [21]. The service states that structural changes over a long period have led to military force being of increased relevance as a political instrument in peace, crisis, and war. Non-military means such as economic power, disinformation, campaigns, surveillance, and computer network operations are alternatives for achieving the same political goals.

Factors linked to Russia and China impact the Norwegian security policy environment the most. Russia has ambitions for great power and has gradually reinforced its defences with a north-western centre of gravity.

> *In August the Northern Fleet, together with the Baltic Sea Fleet, staged the largest naval exercise seen near Norwegian borders since the Cold War. Parts of the Bastion Defence were established all the way down to the North Sea* (Ref. [21], p. 10).

Russia's new defence capabilities includes new submarines, surface vessels, aircraft, and military bases. Operations, exercises as well as testing of sophisticated weapons systems near Norwegian borders will continue, also posing challenges for the environment and security.

It is in both Russia's and China's interest to challenge US dominance in international relations. China seeks superpower status. The so-called New Silk Road initiative is a key component to achieve this (Ref. [21], p. 56). The concept covers communication, public transport and energy infrastructure development, as well domestic and global economic lending, and investments. This includes a Chinese interest also for the Arctic. The Digital Silk Road potentially lays the foundation for a global intelligence capability (Ref. [21], p. 13) Controlling 5G networks, fibre-optic cables and smart city systems enable extensive data collection.

The Norwegian Police Security Service is subordinate to the Ministry of Justice and Public Security. Its main responsibility is to prevent and investigate crimes that threaten national security. The annual threat assessment covers threats from foreign intelligence services and relevant intelligence targets [22]. In addition, it assesses threats from non-state actors in particular from groups and individuals with politically violent ideologies. The Norwegian Police Security Service reports that: (Ref. [22], p. 1)

The most serious threats to Norwegian security are:

- *Foreign intelligence targeted at the government, the Storting (the Norwegian Parliament) and the Armed Forces.*
- *Digital reconnaissance and sabotage of critical infrastructure.*
- *Terrorist attacks carried out by individuals motivated by right-wing extremism or extreme Islamist ideology.*

The political authorities, natural resources, the business sector, defence and emergency planning, and research and development are sectors of great interest to state intelligence activity. The Police Security Service considers the Russian, Chinese and Iranian intelligence services to being able to cause the greatest harm. The service's assessment is that there is an even chance of politically motivated violence committed by right-wing extremists and by extreme Islamists (Ref. [22], p. 3).

The Norwegian National Security Service is a cross-sectoral professional and supervisory authority within the protective security services. It is responsible for preventative national security, and advises and supervises the safeguarding of information, objects, and infrastructure of national significance [18]. In addition, the service has a national responsibility to detect, alert and coordinate responses to serious Information and Communication Technology (ICT) attacks. The directorate is subordinate to the Ministry of Justice and Public Security, but also reports to the Ministry of Defence. The annual risk assessment covers espionage, sabotage, acts of terror and other serious incidents. The National Security Service emphasises digital threats and risks. In the 2020 risk report, the following factors are highlighted (Ref. [18], p. 5):

- Society's dependence on electronic communications and satellite-based services increases, and the society is very dependent on a resilient power supply.
- The dependence of digital infrastructures and international supply chains increases. Trans-border interdependencies may be cost-efficient for enterprises, but complexity and lack of transparency are challenging.
- Strategic purchases, investments and influence using various means could threaten national security. The Security Act gives the Government a mandate to prevent or demand conditions for investments in Norwegian enterprises to safeguard national security.

The COVID-19 crises led to the shutdown of the Norwegian society from 12 March 2020 lasting several months. The authorities struggled to find a balance between preventing further increase of COVID-19 infections and at the same time sustaining vital societal functions. The National Security Service warns that the crisis also may cause additional risks to national security. Threat actors may take advantage of a complex news picture to spread fake news and utilize an active influence strategy. Many have worked from home. This has led to widespread use of digital platforms for sharing information and conducting meetings, increasing digital vulnerabilities as well as straining the electronic communications infrastructure (Ref. [18], p. 7).

The Directorate for Civil Protection is responsible for maintaining an overview of risks and vulnerabilities in Norwegian society and reports to Ministry of Justice and Public Security. Since 2011, it has published risk analyses of scenarios constituting major incidents that society should be prepared to handle. Natural events, major accidents and deliberate acts are analysed. The time perspective is longer than for the annual assessments published by the three intelligence and security services.

The Directorate for Civil Protection has categorised the incidents in 16 risk areas and analysed in total 25 scenarios. A short version of all scenario analyses is presented in a report published in 2019 [4]. Table 6-1 gives an overview of the risk areas and the concrete scenarios. The Directorate for Civil Protection has published more detailed risk analyses for most of these scenarios. The purpose is to inform stakeholders and the public concerning the wide spectrum of threats, hazards and risks that could occur in Norway. Responsible authorities and private enterprises should consider these as a basis for emergency prevention, planning, and response. The scenario analyses serve as inspiration for risk and vulnerability analyses at the central, regional, and local levels as well as for risk assessments for cross-sectoral vital functions and critical infrastructures.

The pandemic scenario scores high on likelihood as well as societal consequences. The two scenarios that scores highest on the combined risk are pandemic and failure of supply of pharmaceuticals (Ref. [4], p. 14). Pandemics occur every 10 to 30 years. The health authorities and the Directorate for Civil Protection have

for many years stated that it is not a matter of "if" we will have a pandemic outbreak of an infectious disease, but "when", thereby warning Norwegian authorities and the public that a COVID-19 type crisis would occur eventually.

Table 6-1: Risk Areas and Scenarios Analysed by the Directorate for Civil Protection. Based on Ref. [4].

Risk Area	Scenarios
Extreme weather and flooding	Storm in the Oslo Fjord Flooding of the rivers Lågen and Glomma Flooding due to torrential rain in city
Avalanches	Mountain slide in Åknes Avalanche of quick clay in city
Infectious diseases	Pandemics in Norway Food transmitted infection Disease outbreak caused by antimicrobial resistance
Wildfires	Three concurrent wildfires
Space weather	Sun storm
Volcanic activity	Volcanic eruption in Iceland
Earthquakes	Earthquake in city
Chemical and explosive incidents	Fire in tanker harbour in city Large-scale gaseous emission from industrial facility
Nuclear accidents	Nuclear accident
Off-shore accidents	Oil and gas blowout
Transport accidents	Ship collision on the West Coast Fire in vehicular tunnel
Failing of supplies	Long-lasting rationing of electricity Global failing of supply of grain Failure of supply of pharmaceuticals
Politically motivated violence	Terrorist attack in city
Violence motivated by revenge	School shooting
Security policy conflicts	Hybrid attack on Norway
Digital attacks	Digital attack against financial infrastructure Digital attack against electronic communications infrastructure

6.2.2 National Objectives and Priorities

The previous section focussed on threats and hazards. This section presents the national objectives and priorities to prevent, prepare for and handle these threats with emphasis on civil-military cooperation. Propositions and White Papers to Parliament, and subsequent political decisions, convey national strategies to safeguard state security and societal security.

Every four years, the Government issues a White Paper on societal security that presents the Government's policy on public security. It constitutes the national public security strategy for the coming four years. The Ministry of Justice and Public Security has a coordinating role for public security, thus is responsible for this White Paper. The Government also issues the Long Term Defence Plan on a quadrennial basis. Since 2004, upon establishment of the modernised total defence concept, the Ministry of Defence and the Ministry of Justice and Public Security have issued these documents the same year.

6.2.2.1 Long Term Defence Plan

The Ministry of Defence published the most recent Long Term Defence Plan on 16 October 2020 [14]. It emphasises that the overall state security objective is to protect and defend the state's existence, sovereignty, democracy, and political freedom of action against any pressure or attack (Ref. [13], p.4) Norway's defence concept encompasses national defence, the collective defence within the framework of NATO, and bilateral support and reinforcement arrangements with close allies.

Due to increasing threats, challenges and vulnerabilities investments in defence and security is a priority of the Norwegian Government. The emphasis is put on continuing building Norwegian Armed Forces as a more joint, robust, interoperable, resilient, and ready force. The Armed Forces is the key instrument of power to protect and defend Norway. The nine tasks of the Norwegian Armed Forces are (Ref. [13], p.4):

1) Ensure credible deterrence based on NATO's collective defence.
2) Defend Norway and allies against threats, aggression, and attacks, within the framework of NATO's collective defence.
3) Prevent and manage incidents and security crises, including facilitating allied support.
4) Ensure national situational awareness in support of decision-making through surveillance and intelligence.
5) Safeguard Norwegian sovereignty and sovereign rights.
6) Exercise Norwegian authority in designated areas.
7) Participate in multinational crisis management, including peace operations.
8) Contribute to international security and defence cooperation.
9) Contribute to societal security and other key societal tasks.

The Government states: "The complexity of threats and risks requires stronger and more flexible civil-military cooperation" Ref. [13], p.2) Building resilience and civil preparedness shall strengthen the ability of the nation to withstand and recover from attacks and incidents, including hybrid threats. A modern total defence framework is crucial for the defence of Norway. It lays the foundation for relevant civilian assets to support the national Armed Forces as well as allied defence efforts during peacetime, crisis, and armed conflict. Section 6.3 gives more information.

6.2.2.2 White Paper on Public Security

The public security White Paper from December 2016 accentuates eight core areas in the Government's work, of which one is on civil-military cooperation and total defence (Ref. [15], pp. 24-26). The Government will present the next White Paper on public security during the autumn of 2020. Although the current public security strategy is four years old, one can expect the emphasis on civil-military cooperation and total defence to be continued and further developed. This as a priority area of the Long Term Defence Plan for the period 2021 – 2024 and the content of the two documents are closely coordinated.

The 2016 public security White Paper urged for strengthening civil-military cooperation, both nationally and within NATO in the period 2017 – 2020. A key objective has been to improve the support from the civil society to the Armed Forces in security crises and armed conflict. The authorities decided to ensure the establishment of plans for civil support, also for supporting allied reinforcement. Further, the strategy was to adapt cooperative and emergency bodies to handle challenges of crises and armed conflict and integrate civil support to Armed Forces in training and exercises.

Secondly, the public security strategy was to improve the Armed Forces' support to civil society by establishing new regulations for the Armed Forces' support to the police and conduct sufficient training in counterterror. The police and the Armed Forces should also complete the plans and training for securing critical objects.

The third priority area in the 2016 public security strategy is to support civil preparedness efforts in NATO and ensure that Norway follows up developments in NATO. At the NATO Summit in July 2016, the member states pledged a commitment to enhance resilience against the full spectrum of threats. The member states highlighted that: "Resilience is an essential basis for credible deterrence and defence and fulfilment of the Alliance's core tasks" [19]. The Alliance established seven baseline requirements to improve civil preparedness, strengthening continuity of government, continuity of essential services and security of critical infrastructures [20]. The Norwegian Government established a four-year Total Defence Programme to ensure a comprehensive approach to developing the total defence and fulfilling NATO's seven baseline requirements (Ref. [13] p. 26). Section 6.3.3 describes the organisation of this programme.

6.3 THE TOTAL DEFENCE CONCEPT

This section presents the total defence concept today, as well as a short historic summary of how the focus of the concept has shifted since Norwegian authorities introduced it after the Second World War. Then, the section explains the important interconnection between state and societal security in Norway, and that resilient vital societal functions are a prerequisite for both. Last, the section describes the four-year Norwegian Total Defence Programme. This section is based on and a partial translation of two book chapters by the author [5], [6].

6.3.1 Total Defence Concept Today and Short Historic Background

The Norwegian comprehensive defence system or whole-of-government approach to crisis management is denoted the "total defence concept". In short, the concept means that all available actors and resources, military as well as civil, should cooperate to prevent, prepare, handle, and recover from crises. In the following, a short historic background is given (Ref. [5], p.64-67).

The Government established the concept after the Second World War to ensure the full mobilisation of the society to defend the nation against an existential threat. During the entire Cold War era, the main emphasis of the concept was to mobilise all available resources for the defence of the nation against an armed attack. This meant that the total defence focus was on civil support to the Armed Forces and civil preparedness in times of war.

From the 1990s, after the end of the Cold War, a broader and more diverse risk picture emerged. Pandemics, industrial and natural catastrophes, transport accidents, terrorism and cyberattacks replaced the dominating fear of nuclear war. The 1990s marked the restructuring of civil protection to also prevent and deal with crises in peacetime when needed. The civil preparedness resources should complement ordinary emergency preparedness when these were not sufficient.

The restructuring and streamlining of civil preparedness continued in the period leading up to the year 2000. From 2000, a change in civil contingency planning occurred. The Government introduced the concept of societal security, merging ordinary emergency preparedness in peacetime with civil preparedness for crisis and war. The purpose was to utilize all of society's resources in both peace and war in a holistic way, also military resources. Hence, the focus gradually shifted towards military support to the civil society in crises. As a result, the government modernised and broadened the total defence concept in 2004 to include also military support to crisis management in peacetime crises. The wording of the total defence concept from 2004 is the same today encompassing mutual civil-military support and cooperation to deal with all types of crises (see definition in Section 6.1.1).

In subsequent years, the domestic priority was emergency preparedness and infrastructure security in peacetime. The Norwegian Armed Forces' focus and engagement was international military operations, first in Kosovo, then in Afghanistan. State security to deter and defend against an external territorial threat and preparations for security policy crisis and armed conflict was not considered as important.

This changed around 2008 – 2010, when the Norwegian planning for national defence, including also civil support to the military, gained attention and became a priority of national authorities. The last decade Norwegian authorities have prioritised re-establishing and renewing total defence planning for security crises and armed conflict.

The short historic summary of the evolution of the total defence concept shows that it has changed because of trends and developments in the security policy situation and perception of threats. Today, the overall objective is a balanced approach to civil-military cooperation within the total defence framework encompassing both civil support to the Armed Forces in crises and armed conflict, as well as military support to civil crisis management in peacetime. Armed Forces' operational capability inherently rests on civil support and civil infrastructures and services. All types of severe crises endangering people's lives or health can prompt military involvement if responsible authorities request military assistance and the military possesses appropriate resources. The next section focusses in civil-military interdependencies.

6.3.2 Civil-Military Interdependencies

In Norway, societal security covers protection against all serious situations, ranging from peacetime accidents to situations that threaten the security and independence of the state, that is, state security. Societal security efforts must ensure resilience of important functions and infrastructures in crises. To systematize the work, the authorities have defined 14 cross-sectoral critical societal functions and areas and appointed a lead minister for each function (Ref. [16], pp. 34-36). In addition, other ministries and a many public and private actors have a partial responsibility for the functions. *Vital (or critical) societal functions* are those functions that society cannot do without for more than seven days or less without endangering the security or safety of the population (Ref. [3], p. 8). The Ministry of Justice and Public Security's latest budget proposition to Parliament gives the current list of vital societal functions. It includes amongst other functions, law and order, health and care, transport, electronic communications network and services, defence, i.e., the functions that ensure the citizens' safety and security as well as the infrastructures that constitute the backbone of a functioning society.

On January 1, 2019, a new Security Act entered into force. The purpose of the law is to safeguard Norway's sovereignty, territorial integrity and democratic governance and other national security interests and to prevent, uncover and counteract security threats [2]. The national security interests are divided into the following five categories (Security Act §1-5):

- The activities, security, and freedom of action of the highest state bodies.
- Defence, security, and emergency preparedness.
- Relations with other states and international organisations.
- Economic stability and freedom of action.
- The basic functionality of society and the basic security of the population.

The Ministry of Defence states that second category "defence, security and emergency preparedness" includes the Armed Forces and the defence sector with supporting functions in a total defence context (Ref. [11] p. 34). The defence is directly dependent on civilian contribution through the total defence; thus, the total defence is fundamental to the military response capability.

The fifth category of national security interests is "the basic functionality of society and the basic security of the population" (Security Act §1-5). The Ministry of Defence emphasises that the Security Act provisions will also apply to infrastructure and services that do not directly support the Armed Forces but are crucial for civil society to function and thereby important for overall preparedness and defence capabilities (Ref. [11] p. 35). This implies a "limited extension of the scope of the Act" as compared with the previous one (Ref. [11] p. 37). It remains to see how extensive this expansion will be.

The Security Act defines *basic national functions* as:

> *[…] services, production, and other forms of activity that are of such importance that a complete or partial loss of function will have consequences for the state's ability to safeguard national security interests.* (Security Act § 1-5.)

The Security Act is primarily a state security law, but also intervenes in the field of societal security (Ref. [6], pp. 406-419). There are, in part, interdependencies and overlaps between the functions and values that are crucial for state security (basic national functions) and those functions that are critical for societal security (critical societal functions). This is a consequence of relationships and mutual dependencies related to the delivery of goods, services, and emergency functions in society. Fuel, food, water, transport, health care and more is provided through resilient critical social functions. In principle, features such as electronic communication, power supply and satellite-based services should be always available to meet both military and civilian needs. The general societal security work is thus a basis for national security interests and defence capabilities.

6.3.3 Total Defence Programme

In 2016, the Ministry of Justice and Public Security established a four-year Total Defence Programme for the period 2017 – 2020 (Ref. [15], p. 26). The purpose is to further develop the total defence and increase the resilience of critical societal functions by following up NATO's basic requirements and contributing to civil support to the Armed Forces in planning and exercises. The programme is closely linked to the work within critical societal functions, thereby placing the programme within the framework of the public security work and avoiding parallel processes. The programme consists of ten projects, and the project responsibility at the ministerial level corresponds to the main responsibility for critical societal functions.

Table 6-2 provides an overview of NATO's seven baseline requirements and the projects in The Total Defence Programme. The table also gives an overview of the link to the corresponding Norwegian critical societal functions. As can be seen, two of NATO's requirements are divided into two separate projects. This is due to the Norwegian division of overall responsibility between the ministries. In addition to the projects that correspond to NATO's requirements, the Directorate for Civil Protection leads a project to develop the civil support to the Armed Forces.

The four-year programme ends in 2020. Information from responsible project owners on main achievements is not yet available. The exception is the project led by the Directorate for Civil Protection. A main activity of this project has been civil-military preparations and participation in the NATO exercises Trident Javelin in 2017 and Trident Juncture in 2018. Main experiences from this work are presented in Section 6.4.3.

Table 6-2: The Norwegian Total Defence Programme is a Four-Year Programme Consisting of Ten Projects. The aim is to follow up on NATO's seven baseline requirements and enhance the resilience of critical societal functions. The table is based on Ref. [5].

The Total Defence Programme (2017 – 2020)			Corresponding Critical Societal Function in Norway
NATO's Seven Baseline Requirement	**Project**	**Responsible Entity**	
Assured continuity of government and critical government services	Assured continuity of government and critical government services	Ministry of Justice and Public Security	Governance and crisis management
Resilient energy supplies	Resilient energy supplies – Electricity and gas	Ministry of Petroleum and Energy	Power supply
	Resilient energy supplies – Fuel supply	Ministry of Trade, Industry and Fisheries	Security of supply
Ability to deal effectively with uncontrolled movement of people	Ability to deal effectively with uncontrolled movement of people	Ministry of Justice and Public Security	Law and Order
Resilient food and water resources	Food supply	Ministry of Trade, Industry and Fisheries	Security of Supply
	Water supply	Ministry of Health and Care Services	Water supply and sewage
Ability to deal with mass casualties	Ability to deal with mass casualties	Ministry of Health and Care Services	Health and care
Resilient civil communications systems	Resilient civil communications systems	Ministry of Local Government and Modernisation	Electronic communications network and services
Resilient transport systems	Resilient transport systems	Ministry of Transport	Transport
	National Project		
	Further develop civil authorities' and civil society's support to the Armed Forces	Directorate for Civil Protection	

6.4 NATIONAL AND INTERNATIONAL INTEROPERABILITY

This section introduces the national emergency preparedness and response system, the most important total defence legislation, roles and responsibilities of key actors and total defence cooperative fora.

6.4.1 National Emergency Preparedness and Response System

Norway bases her defence and security on collective defence in line with the NATO Treaty. In the escalation to and in the event of a conflict, it is crucial for the Norwegian authorities to involve NATO and coordinate political decisions with NATO and allied nations. NATO has established a common crisis management system that provides a unified platform for decision-making and command and control of military forces. NATO encourages member states to develop a national crisis management system that corresponds to NATO's system. Norway has therefore developed a National Emergency Preparedness and Response System comprised of a Civil Preparedness System and the Emergency Preparedness System for the Defence Sector (Ref. [10] pp. 26-27). Both have the same structure as the NATO Crisis Response System (NCRS) but are adapted to Norwegian conditions.

The contents are procedural descriptions, actions and measures that authorities at various levels may implement according to the situation and to achieve an appropriate increase in emergency preparedness. The scope of the system is:

1) Cross-sectoral crises in peacetime caused by serious intentional events or threats thereof, such as terrorist or cyberattacks; and
2) Crises with a security policy dimension and armed conflict or threats of such.

Natural disasters and technological accidents are outside the scope of this system and are subject to other contingency plans.

The system is subject to an annual audit. The National Emergency Preparedness and Response System affects all ministries and subordinate agencies, and they have to prepare contingency plans based on the system. The County Governor is responsible for coordinating underlying civil planning at the regional level. Ensuring the existence of such plans are part of The Total Defence Programme.

6.4.2 Total Defence in Peacetime Crises

This sub-section presents the publicly organised rescue service, which is a cornerstone of Norwegian search and rescue to save lives. Then, the section introduces the Armed Forces support to the police, as regulated by law and regulations. Finally, some examples of civil-military crisis cooperation are mentioned.

6.4.2.1 The Publicly Organised Rescue Service

The principle of cooperation is the foundation for the publicly organised rescue service [25]. "All governmental agencies, including the Norwegian Armed Forces, are obliged to participate in rescue operations with appropriate and available resources" (Ref. [10], pp. 17-18). Private and voluntary resources also play an important role and assist the public rescue service within their areas of expertise. There are three emergency telephone numbers in Norway: fire rescue centre (110), police (112) and emergency medical coordination centre (113), respectively.

The Ministry of Justice and Public Security is administratively responsible for land-, sea and air rescue services. The operation of the rescue services is organised by two Joint Rescue Coordination Centres, for the south and north of Norway, respectively, and twelve local rescue centres located in the regional Police districts. The Governor of Svalbard is responsible for the local rescue centre within its jurisdiction. The Joint Rescue Coordination Centres are directly responsible for sea and air rescue operations. The local Police commissioners lead the local rescue centres and is responsible for land rescue operations.

The Norwegian Armed Forces play an important role in the rescue service and assist the civil society in accidents and disasters. The Norwegian Joint Headquarters handles requests for assistance and coordinate military contributions.

The rescue helicopters are important resources for the rescue service. The Government owns the helicopters, the Ministry of Justice and Public Security has the operational and budgetary responsibility. The Norwegian Armed Forces train, educate, and man the rescue helicopters.

Voluntary rescue and emergency preparedness organisations also play an important role. The Norwegian Professional Rescue Organisation's Forum is an umbrella organisation for many of the voluntary organisations. The Forum has one representative in the rescue leadership in each police district.

6.4.2.2 The Armed Forces Assistance to the Police

The Government laid down a new instruction for the Armed Forces' assistance to the police on 19 June 2017 [24] The new instructions are simplified and shortened and will ensure that decisions on assistance from the Armed Forces to the police can be taken as quickly as possible in a crisis. The objective of the instruction is to facilitate even better cooperation between the police and the Armed Forces. The new assistance instructions mean that the previous distinction between enforcement assistance and general assistance is removed. Now, all decisions on requesting and granting assistance will be taken in the agencies, usually at the Armed Forces Joint Operational Headquarters and in the relevant police district or the Police Directorate. The ministries exercise a reactive management right.

The Armed Forces can assist the police in the following situations according to the instruction § 3 and the Police Act § 27 a [24]:

1) *Prevention and control of attacks that are of particularly harmful or extensive nature, including guarding and securing objects and infrastructure;*
2) *The search and seizure of persons who may seriously endanger human life and health or material social interests; and*
3) *Accidents, natural disasters, and the like in order to protect people's lives and health, property and to maintain peace and order.*

6.4.2.3 Some Examples

There are numerous examples where the military assist civil authorities in crisis management. The Home Guard has assisted civilian emergency response authorities in events within several of the risk areas in Table 6-1. At the 1995 Vesleofsen flooding, the Home Guard assisted in carrying sandbags to reduce the consequences of the flood, especially in the town of Lillestrøm.

After the bomb attack against the governmental quarter on 22 July 2011, the Home Guard assisted in securing, among other things, the Parliament. In the forest fires that ravaged southern Norway in 2018, the Home Guard assisted with monitoring and extinguishing the fire when firefighters and the Civil Defence needed relief.

During the COVID-19 pandemic in 2020, the Home Guard assisted the police with border control at the border crossings to Sweden and Finland. Home Guard personnel were given limited police authority but did not carry weapons. The Home Guard also assisted the police at Oslo International Airport Gardermoen providing information on the authorities' COVID-19 measures and regulations to arriving passengers from abroad.

6.4.3 Total Defence in Security Policy Crises and Armed Conflict

One may argue that the Norwegian revitalisation of the total defence planning for security policy crises and armed conflict culminated in the NATO Exercise Trident Juncture 2018 (TRJE18). Experiences and lessons learned from this exercise conveys a mirror of the status.

During the autumn of 2018, Norway hosted the NATO Exercise Trident Juncture 2018 (TRJE18). The exercise aimed to train collective defence and certify NATO's Response Force 2019. The purpose was to demonstrate NATO's will and capability to defend allied nations, resist, and defeat enemy forces. A key objective for Norway was to train large-scale receipt of allied reinforcement forces, as well as to test the national concept for Host Nation Support, national contingency plans, and the civil-military cooperation in accordance with the total defence concept. TRJE18 had two parts, a Live Exercise, and a Command Post Exercise. Norway conducted the national exercises Polaris/Gram and the National Health Exercise 2018 in conjunction with TRJE18.

The Ministry of Defence and the Ministry of Justice and Public Security tasked the Norwegian Defence Research Establishment (FFI) to assess TRJE18. FFI assessed to what extent the exercise contributed to Norwegian security, the national benefits of the exercise, the attainment of exercise objectives and essential lessons learned [7]. The perspective of the assessment was a national one, and the focus was on civil-military cooperation.

Endregard et al. [7] concluded that TRJE18 has contributed to Norwegian security in several ways. The exercise has drawn the attention of the Alliance to the High North. Allied Nations have gained knowledge and experience in operating in Norwegian areas. NATO and Norway as a host nation also balanced the consideration of maintaining the High North as a region of low tension by early warning, openness, transparency, and adherence to international treaties. The exercise demonstrated NATO's will and ability of collective defence and thereby contributed to deterrence. A well-functioning cooperation between military and civilian total defence actors concerning Host Nation Support is a prerequisite for allied support. TRJE18 contributed to strengthen this cooperation.

The national benefit of TRJE18 was substantial. Many lessons were learned, which are currently being pursued. TRJE18 enhanced Norway's visibility and recognition within NATO. The Norwegian defence trained together with NATO. Norway tested the concept for Host Nation Support, parts of national contingency plans, and performed real life Host Nation Support. TRJE18 enhanced the competence in interoperability for information- and communication systems both nationally and in NATO. TRJE18 increased the knowledge concerning legislation, instructions, legal authority, roles, and responsibilities. The exercise catalysed enhanced interaction within the total defence model and vitalised total defence development.

The National Health Exercise increased the health services' ability to handle mass casualty and evacuation situations, as well as the health sector's cooperation with the military, NATO, non-governmental organisations, and other key actors. For the most part, exercise participants achieved their respective exercise objectives.

TRJE18 was time- and resource-consuming but gave the total defence a lift. The main conclusions from the TRJE18 for the Norwegian total defence in a civil-military perspective are:

- This was the largest total defence exercise and operation since the 1990s in Norway.
- TRJE18 was well planned and the foundation for learning and further improvements.
- It was truly a cross-sectoral exercise in Norway where military, civilian and private actors at various levels participated.
- Norway experienced receipt, transport, and support of allied forces in practice.
- A new Host Nation Support concept was developed, exercised, and revised after the operation.
- Involvement of civilian competent authorities (liaisons) was a success.
- Relevant strategic and principal issues were discussed at the central level and are being followed up.

TRJE18 has been a main driver for revitalising "total defence" planning and engagement. The same structures and mechanisms were used as for crisis management in other severe crises. Hence, it is safe to argue that TRJE18 has enhanced national crisis management ability in general.

However, it is important to note that several issues were not part of the exercise, for instance use of mechanisms and councils to ensure security of supplies. The exercise required a lot of time, effort, and resources across the total defence actors. Many individuals became highly skilled in the course of the exercise. It is important to transform lessons learned to change and improvements and institutionalise knowledge and competence.

6.5 CHALLENGES OF IMPLEMENTATION

Actors in the total defence, like everyone else in society, depend on a variety of societal functions and services, some of them critical to the performance of their duties. Since the National Emergency Preparedness and Response System got its design, there has been dramatic changes in society. The public sector has been reorganised and privatised, and businesses and infrastructures have become more international. Most of the goods and services production today is on private hands independent of national boundaries and is subject to considerable competition. The private sector and the business sector have therefore increased their importance as a premise for national preparedness and the total defence.

More than ever, defence and national preparedness are dependent on private-public cooperation and the secure supply of goods and services in an international framework (Ref. [8], pp. 100-116). At the same time, technology development is moving fast, for example with regard to increasing digitalisation. ICT-based systems and services are crucial. Both value chains and ownership relationships change faster than ever. In this fluent and uncertain landscape, it is uncertain how vulnerable the various critical societal functions are to disturbances, sabotage, and direct attacks. This is a challenging situation characterized by rapid change, in particular understanding and having an overview of the technologies and systems the Armed Forces and the Total Defence depend on and their weaknesses and vulnerabilities.

An objective of implementing the new Security Act in Norway is to assure that entities that are of crucial national security importance within critical functions and infrastructures are included under its provisions. This may prove challenging in practice. Parts of critical social functions will most likely be designated as basic national functions. The Security Act with the higher requirements that follow will thus cover businesses that are crucial to these. This becomes demanding due to the complexity of these functions and infrastructures. Private companies, partly with international branches or ownership, increasingly provide civil infrastructure and services. In addition, many Norwegian and foreign players and subcontractors may be involved, and changes may occur quickly. This complicates the security work. Is it a fact that in open democratic nations with an open market-based economy, national autonomy and national governance of infrastructures are no longer possible?

Another key challenge that requires close attention in the further development of the Norwegian Total Defence, is to balance how the civilian support to the military is orchestrated with the compliance with International Humanitarian Law. The Geneva Conventions and Additional Protocols aim to protect civilians in armed conflict and war. Civilian support to the Armed Forces may challenge the clear distinction between military forces and civilians, thus possibly impairing the protection of civilians. Hence, planning for civilian support to the military requires close dialogue and in-depth considerations in order to secure protection of civilians and Norwegian Armed Forces Compliance with International Humanitarian Law.

6.6 FUTURE DEVELOPMENTS AND ONGOING DISCUSSIONS

The importance of the contribution of civilian actors has increased as the military support structure and the deployment of services in the Armed Forces, as well as privatization and efficiency in society in general, have increased. The authorities have decided further to develop the total defence. The need for civilian support for the Armed Forces is recognised, and the Armed Forces and civilian agencies have come a long

way in developing the necessary planning work. Not least, the Total Defence Programme and the NATO exercise Trident Juncture in 2018 helped accelerate the work. However, the work will never be complete. It requires constant attention.

In today's society, goods and services are privatised, globalised, and based on just in-time production and reduced stocks. The modern digitalised society is critically dependent on electronic communications, electric power supply and satellite-based services. Extensive electrification is underway in the transport sector. New technologies such as artificial intelligence, big data, quantum computers and autonomous systems contribute to so rapid changes that it is difficult to keep track. This will affect total defence planning and civil-military crisis management. Key challenges for civil-military emergency preparedness and response are adapting quickly enough and ensuring that society's critical functions are sufficiently resilient.

Different types of exercises will be central to maintaining existing competence, further developing and institutionalising knowledge of each other and developing cooperation and a flexible crisis management ability of key stakeholders. The Armed Forces must continue to increase their knowledge of, and cooperation with, civil society at all levels. Civil authorities and actors must, prioritise planning and crisis management exercises together with the Armed Forces. Total defence contingency planning, competence enhancement and exercises need to be a continuous work, not subject to fluctuations based on the security policy situation and other events. The Total Defence Programme ends in 2020, but the development of a flexible total defence, based on and adapted to the contemporary society is a continuous project.

6.7 REFERENCES

[1] "Instruks for statsforvalteren og Sysselmesteren på Svalbard sitt arbeid med samfunnssikkerhet, beredskap og krisehåndtering" [Instructions for the County Governor and the Governor of Svalbard's work with societal security, emergency preparedness and crisis management] of 19 June 2015". https://lovdata.no/dokument/INS/forskrift/2015-06-19-703?q=fylkesmannens%20beredskap

[2] Act of 1 June 2018, No. 24 on National Security (Security Act), https://lovdata.no/dokument/NL/lov/2018-06-01-24.

[3] Directorate for Civil Protection (2017), "Vital Functions in Society. What functional capabilities must society maintain at all times?".

[4] Directorate for Civil Protection (2019), «Analyse av krisescenarioer 2019», (English title: Analyses of Crisis Scenarios 2019), (In Norwegian, https://www.dsb.no/globalassets/dokumenter/rapporter/p1808779_aks_2018.cleaned.pdf, Accessed 29 Feb 2020.

[5] Endregard, M. (2019), «Totalforsvaret i et sivilt perspektiv», (English title: Total Defence in a Civil Perspective.) In P.-M. Norheim-Martinsen (Ed.) Det nye totalforsvaret. (English title: The New Total Defence.) Oslo: Gyldendal. pp. 64-67. (In Norwegian).

[6] Endregard, M. (2020), «Totalforsvaret – samfunnet i væpnet konflikt», (English title: Total Defence – society in armed conflict.) In A.K. Larssen, and G.L. Dyndal (Eds.) Strategisk ledelse i krise og krig. Det norske systemet. (English title: Strategic Leadership in Strategic leadership in crisis and war. The Norwegian system.) Oslo: Universitetsforlaget. pp. 406-419.

[7] Endregard, M., Elstad, A.-K., Siedler, R. E., Tønsager, J., Brattekås, K. and Åtland, K. (2019), «Vurdering av Trident Juncture 2018», (English title: Assessment of Trident Juncture 2018). FFI-rapport 19/01791. Kjeller: Norwegian Defence Research Establishment. (RESTRICTED)

[8] Listou, T. (2019), «Totalforsvaret og kommersielle aktører – den doble logistikkutfordringen», In P.-M. Norheim-Martinsen (Ed.) Det nye totalforsvaret. (English title: The New Total Defence.) Oslo: Gyldendal, pp 100 – 116. (In Norwegian).

[9] Members of the Government. https://www.regjeringen.no/en/the-government/solberg/members-of-the-government-2/id543170/, Accessed 26 Mar 2020.

[10] Ministry of Defence and Ministry of Justice and Public Security (2018), "Support and cooperation. A description of the total defence in Norway, https://www.regjeringen.no/contentassets/5a9bd774183b4d548e33da101e7f7d43/support-and-cooperation.pdf, Accessed 28 Feb 2020.

[11] Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen)" [Instructions for the ministries' work on societal security] of 1 September 2017. https://lovdata.no/dokument/INS/forskrift/2017-09-01-1349?q=Samfunnssikkerhetsinstruksen

[12] Ministry of Defence (2017), «Lov om nasjonal sikkerhet (sikkerhetsloven). Prop. 153 L (2016-2017)». (English title: Act on National Security (Security Act) Proposition to Parliament). (In Norwegian).

[13] Ministry of Defence (2020), "The defence of Norway. Capability and readiness. Long term defence Plan 2020. English summary". https://www.regjeringen.no/contentassets/3a2d2a3cfb694aa3ab4c6cb5649448d4/long-term-defence-plan-norway-2020–-english-summary.pdf, Accessed 17 Apr 2020.

[14] Ministry of Defence (2020), «Prop. 14 S (2020 –2021) Evne til forsvar – vilje til beredskap. Langtidsplan for forsvarssektoren». (English title: Long term defence plan), https://www.regjeringen.no/no/dokumenter/prop.-14-s-20202021/id2770783/.

[15] Ministry of Justice and Public Security (2017), "Meld. St. 10 (2016-2017) Report to the Storting (White Paper). Risk in a safe and secure society. On public security. Executive Summary", https://www.regjeringen.no/contentassets/00765f92310a433b8a7fc0d49187476f/en-gb/sved/stm201620170010000engpdfs.pdf, Accessed 28 Feb 2020.

[16] Ministry of Justice and Public Security (2019), «For budsjettåret 2020. Prop. 1 S (2019 – 2020) ». (English title: For the Fiscal Year 2020. Proposition to Parliament). (In Norwegian).

[17] Ministry of Justice and Public Security (2020), «Meld. St. 5 (2020–2021). Samfunnssikkerhet i en usikker verden», (English title: Public Security in an Uncertain World.), https://www.regjeringen.no/no/dokumenter/meld.-st.-5-20202021/id2770928/.

[18] National Security Service (2020), «Risiko 2020», (English title: Risk 2020) (In Norwegian), https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm-risiko-2020.pdf, Accessed 19 Jun 2020.

[19] NATO (2016), "Commitment to enhance resilience". Press Release. 8 July 2016. https://www.nato.int/cps/en/natohq/official_texts_133180.htm, Accessed 28 Feb 2020.

[20] NATO (2016), "Warsaw Summit Communiqué, 9. July 2016", https://www.nato.int/cps/ic/natohq/official_texts_133169.htm?selectedLocale=en, Accessed 30 Aug 2020.

[21] Norwegian Intelligence Service (2020), "Focus 2020. The Norwegian Intelligence Service's assessment of current security challenges", https://forsvaret.no/presse_/ForsvaretDocuments/Focus2020-web.pdf, Accessed 18 Jun 2020.

[22] Police Security Service (2020), National Threat Assessment 2020, https://www.pst.no/globalassets/artikler/trusselvurderinger/national-threat-assessment-2020-pst.pdf, Accessed 18 Jun 2020.

[23] Royal Decree of 10 March 2017. "Responsibility for civil protection and emergency preparedness in the civil sector at a national level and the Ministry of Justice and Public Security's coordinating role related to civil protection and emergency preparedness and ICT Security".

[24] Royal Decree of 16 June 2017. «Instruks for Forsvarets bistand til politiet (Bistandsinstruksen)», (English title: Instructions for the Armed Forces' Assistance to the Police). https://lovdata.no/dokument/INS/forskrift/2017-06-16-789?q=instruks%20forsvarets%20bistand%20til%20politiet.

[25] Royal Decree of 19 June 2015, «Organisasjonsplan for redningstjenesten», (English title: Organization Plan for the Rescue Service.) https://lovdata.no/dokument/INS/forskrift/2019-12-06-1740?q=redningstjenesten.

[26] Royal Decree of 24 June 2005, "Instructions to the Directorate for Civil Protection and Emergency Preparedness for its coordination roles".

[27] Statistics Norway (2020), https://www.ssb.no/en, Accessed 26 Mar 2020.

Chapter 7 – TURKISH CASE STUDY

Sait Yılmaz
Esenyurt University
TURKEY

7.1 INTRODUCTION

Turkey's geography, history, religion, and culture have positioned it as a centre of gravity along the east-west and north-south axes. By virtue of its geography, the turmoil in the Eastern Mediterranean and the Middle East will directly affect Turkey and threaten its security. Turkey has a central position in Eurasia at the confluence of maritime, land, and air transportation routes. Recent convulsions in the surrounding geography are expected to last for the foreseeable future with unpredictable consequences. The aim of this case study is twofold:

- To describe the Turkey's approach to civil-military cooperation within the evolving framework of Comprehensive National Defence.
- To ensure that the Nation is capable of coping with a wide array of threats from natural and human-made disasters as well as hybrid threats to use military force.

7.1.1 The Concept of CND in National Strategic Documents

From the international perspective, the Turkish Armed Forces have long standing experience for interoperability beginning with an active role in the Korean War in the 1950s. Turkey has taken major roles in international operations both in NATO and other international coalitions as mandated by the United Nations – in particular NATO Operations in Bosnia and Herzegovina (1996), Kosovo (since 1999), Afghanistan (since 2002) or international coalitions under the UN umbrella in Somalia (1993), Bosnia and Herzegovina (1994).

Currently Turkish armed units are operating in three continents and 12 countries with some Turkish military bases in accordance with international agreements. Those countries are: Afghanistan; Albania; Azerbaijan; Bosnia and Herzegovina; Iraq; Kosovo; Lebanon; Libya; Northern Cyprus Turkish Republic; Qatar; Somalia; and Syria.

Since the 1990s, Turkish Armed Forces have developed great interoperability capabilities and doctrines based on their experience in those operations in addition to logistic capacity such as national strategic lift and strategic communication assets.

The Turkish Armed Forces have a constant learning and innovating organization by adapting to rapidly changing conditions in order to bring instant solutions to the theatre.

A glance at the Turkish Armed Forces' recent combat record demonstrates that Turkey's defence policy now extends well beyond its borders. Drones loitering in Syrian airspace, navy frigates along the Libyan coast, Turkish military advisors in Tripoli alongside Government of National Accord (GNA) formations, mountain commando units operating in northern Iraq, and high-ranking Turkish officers in Qatar and Somalia are all common to see now. Overall, the Turkish military is fast becoming an expeditionary actor in league with Ankara's geopolitical worldview.

Turkey's ambitious strategic posture is cantered on three pivots. These are the naval transformation toward a blue-water force; the army's expeditionary warfare concepts married to a growing tendency of resorting to proxy war agents in various battlegrounds from North Africa to the Levant; and expanding forward military bases in different parts of the Turkish *zone d'influence*.

7.1.1.1 Rise of Forward-Bases

Out of Turkey's forward-deployed contingents, those with the highest geopolitical significance include the training mission in Somalia, Turkey's forward-deployed corps in northern Cyprus since its military intervention in 1974, the joint base in Qatar, the special forces and military advisory contingent in Libya and the forward-operating bases in Syria and northern Iraq [18].

Today, the Turkish military advisory missions are going beyond business as usual. Somalia is a good example in this respect. The Somali cadets graduate singing the Turkish Military Academy's anthem [24]. The African nation's commandos are trained by the Turkish Army's elite instructors and take their oaths in the Turkish language. Overall, in the Horn of Africa, Turkey has been rearing a whole new military generation [3].

Turkey's 'dronization' trend has also shaped the overseas basing posture. Ankara deployed surveillance drones to northern Cyprus for the first time since the outset of its decade-long military presence on the island. Likewise, Turkish unmanned aerial vehicles are regularly operating in the Syrian, Libyan and northern Iraqi skies.

7.2 THREAT PERCEPTION, NATIONAL OBJECTIVES, AND PRIORITIES

7.2.1 Threat Perception

In Turkey's case, the identification and continuous reassessment of risks and threats, and the formulation of concepts and strategies, are ensured by the collaboration of relevant institutions: the Ministry of National Defence (MND), Chief of General Staff, National Security Council (NSC), Ministry of Foreign Affairs, National Intelligence Organization (NIO), etc.

The NSC has continued to be the main platform where national security priorities are discussed and determined. The NSC also has been the arena where the National Security Policy Document (NSPD), the so-called Red Book, is prepared. The clout of the NSPD is so dominant that it is referred to as the 'secret constitution' of Turkey because presumably no law can be legislated in contradiction to it.

Full texts of the NSPD and the NSC meeting minutes are not disclosed to the public. Haphazard information on the NSPD leaks to the public every 4 – 5 years when it is renewed, which can give some clues regarding national security priorities [28].

Similarly, after each Council meeting, a press briefing is issued on the NSC website summarizing the main matters that were discussed and outlining the policies that are being followed [14]. These briefings also contain warnings and relay wishes addressed to the international community and neighbouring countries, providing a useful tool to understanding the main elements of military doctrine.

According to "unclassified" national security studies, Turkish national threat perception differs from the Cold War period. Turkey does not identify any country as a direct threat. Due to the uncertain character of the current strategic environment, Turkey has foreseen some risks for concern regarding her national security [9].

State sourced risks are usually listed as the following [12]:

- Regional and ethnic conflicts;
- Political and economic instabilities and uncertainties in neighbouring countries;
- The proliferation of weapons of mass destruction and long-range missiles; and
- Drug smuggling and other illegal trafficking.

Non-state risks are covered as below:

- Transnational separatist terror (the PKK Terror Organization);
- International terrorism (Al Qaeda and ISIS) ; and
- Parallel structures targeting regime stability (FETO).

Other risks for national security:

- National disasters, particularly earthquakes;
- Cyber-attacks;
- Pandemics; and
- Environmental issues.

7.2.2 National Objectives and Priorities

National priorities refer to protecting and preserving Turkish national interests and the sovereign rights of Turkey in compliance with international laws. In that respect, national objectives are generally defined as [6]:

- Survival and security in the Turkish state and society;
- Promoting the economic and social life standards of Turkish people; and
- Preserving and protecting the Turkish national identity.

The Turkish National Security System

The President of the Republic of Turkey is the Supreme Commander of the Turkish Army. The Council of Ministers is answerable to the Turkish Grand National Assembly on matters of National Security (Ref. [7], p.77). However, authority rests with the National Assembly for the declarations of war, sending troops abroad or allowing foreign troops to be stationed in Turkey.

The Ministry of National Defence is authorized to implement security policies as decided by the Council of Ministers.

The Chief of the General Staff is appointed by the President and is responsible to the Prime Minister. The Chief of the General Staff is responsible for the overall command of the Armed Forces, preparation of the Army for war and conducting military operations.

In addition, the National Security Council consists of the President, the Prime Minister, various Ministers and the commanding officers. The council meets every two months in order to discuss national security issues.

Moreover, it is the responsibility of the Minister of the Interior to secure public peace. The police in urban areas, the gendarmerie in rural areas, and the coastguard at sea are tasked with maintaining public security by the Minister of the Interior.

The Principles of the National Security Policy: According to Law No. 2945, National Security involves:

> *The preservation and protection against all kinds of internal and external threats to the constitutional order of the state, her national existence, her integrity and all her political, social, cultural and economic interests and contractual rights in the international arena.*

The elements, “constitutional order, national existence, integrity, national interests and contractual rights” are included in the definition of National Security among the national values of the state having vital importance.

The National Security Policy is defined as follows in Law No. 2945: "It is a policy including the principles related to internal, external and defence type operations determined by the Council of Ministers within the purview determined by the NSC with the objective of providing national security and attaining the national goals."

According to Article 5 of the Constitution, the basic goals and duties of the state are expressed as "To protect the independence and integrity of the Turkish Nation, the indivisibility of the country, the republic and democracy, and to provide for the prosperity, peace and happiness of individuals and the society".

Attaining the highest national interests that can be defined as the "Eternal Existence of the State and the Prosperity of the Nation" through the achievement of the above-mentioned national objectives has also been guaranteed by the National Security Policy [27].

National strategy documents and defence development plans are presented to the parliament by the National Defence Commission. Members of the commission are selected from the Turkish Grand National Assembly following each general election.

7.3 NATIONAL AND INTERNATIONAL INTEROPERABILITY

7.3.1 CND System Implementation

The Ministry of National Defence is the main authority to develop and update the national defence policy in coordination with political and military bureaucracy including the Presidential Office, other ministers of the Cabinet, General Staff and other authorities. This bureaucracy convenes periodically in the form of boards or committees subject to required expertise. There are four main bodies with regard to defence matters [34]:

- The National Security Council and its Secretariat;
- The High Coordination Board of the Defence Industry;
- The Executive Committee of the Defence Industry; and
- The Supreme Military Council.

The Ministry of National Defence publishes a "White Paper" for transparency. The latest White Paper was issued in 2013 [31].

According to the White Paper, Turkish defence policy is naturally defensive and aims to protect and maintain the independence, sovereignty, territorial integrity and vital interests of the country. In this respect, Turkish national policy refers to the following objectives (Ref. [31], p.88):

- To contribute to peace and security and spread the stability in her region and beyond in accordance with the motto of Atatürk, the founder of Turkish Republic; "Peace at home, peace abroad";
- To ensure power balance and produce security and strategy for her sphere;
- To cooperate with other nations in positive relations to deescalate tensions and contribute to fair and standing peace;
- To take all measures necessary to prevent the crisis and conflict; and
- To take part actively in collective defence systems and fulfil all responsibilities assigned to the nation.

Turkey's Military Strategy contains four important matters to ensure support for the specified defence policy (Ref. [32], p. 259):

- Deterrence;
- Military Contribution to Crisis Management and Intervention in Crises;
- Forward Defence; and
- Collective Security.

In line with her national defence and security policy as depicted above, Turkey contributes to the international institutions, alliances and respective states and also makes agreements concerning military cooperation, technical aid and training support within the understanding of collective security.

The following documents are circulated to formulate defence and military policies (Ref. [16], pp.22-23):

- National Security Policy Document (Secretariat of the National Security Council).
- Ministerial Guidance + NATO Strategy.
- National Military Strategy Document (General Staff).
- General Operational Concept Document (General Staff).
- Planning and Programming Directive (General Staff).
- Requirements Document (RD) (Services).
- Force and Armament Proposals (Services).
- Strategic Goal Plans (General Staff).
- Ten Year Procurement Program (General Staff).

Although Turkish Constitutions emphasized the supremacy of civilian authority in the defence sector, elected officials have deliberately given the military exclusive authority on defence matters, until very recently.

Real power in defence policy-making rested in the military so long as civilians allowed it (Ref. [15], Chapters 4, 6) Defence policy concerning crisis situations provides us with the best example. Rather than a military vs. civilian divide, a focus on expertise vs. politics is a more useful tool in analysing which institution has greater weight for defence policy.

7.3.2 Crisis Management Organisation

7.3.2.1 Military Contribution to Crisis Management and Intervention in Crises

When a crisis occurs in the strategic environment, the scope of the situation is set by agenda of National Security Council, which then advises the Cabinet and Presidency. The issue may be taken to the parliament agenda for broader discussion. If there is a need to prompt any military involvement, only the Turkish Grand National Assembly has the authority to send troops and declare war according to Turkish Constitution (Article 92).

In a crisis concerning Turkey's security, for the peaceful solution of the disagreements in conformity with diplomatic, economic and other crisis management measures, one of the most important elements of its strategy is that the Turkish Armed Forces must be ready to contribute to reducing tension, prevent the situation from transforming into armed conflict or otherwise restrict the aggressor.

The Turkish Armed Forces' contribution to international efforts for the solution of crises threatening peace and stability within the United Nations and the Alliances to which it is a party, with respect to making political decisions regarding crises in its region and being ready to preserve, establish and maintain world peace are also in the lead among the duties that cannot be relinquished.

7.3.2.2 Forward Defence

To be able to determine as soon as possible the scope of a probable aggressive situation or when subjected to actual external aggression, the principle of stopping this aggression constitutes the foundation of forward defence.

Under state of emergency conditions, the government appoints special public order units formed within the framework of the State of Emergency Law No. 2935 and appoints military units within the framework of "Martial Law No. 1402", provided that it is ratified by the Turkish Grand National Assembly (TGNA), for providing public order and general security.

To provide effectiveness in the fight against terrorism, responsibility was given to the Ministry of Internal Affairs by the State of Emergency Law No 2935 (a decree having the force of law within the scope of the law), the "State of Emergency Governor's Office" and the "Gendarmerie Public Order Command" were established under the Ministry of Internal Affairs, and sufficient police forces were assigned to them. With this law, the State of Emergency Governor can also use the military forces in the region in the fight against terrorism when necessary. This struggle is carried out completely under the control and management of the legal civilian authority (Ref. [21], pp. 58-62). In this connection, the Prime Ministry State of Emergency Coordination Council and the Internal Security Evaluation Council was established under the chairmanship of the Minister of Internal Affairs and some additional measures were taken.

The place in the state structure of the Turkish Armed Forces (TAF), its representation and use is regulated by the Constitution of the Republic of Turkey. According to the Constitution, the Supreme Military Command is represented in the spiritual authority of the Turkish Grand National Assembly (TGNA).

The Chief of General Staff, as the Commander of the Armed Forces, is appointed by the President and is responsible to the Prime Minister for his duties. The Council of Ministers is responsible to the TGNA for National Security and the preparation of the Armed Forces for the defence of the country. However, the authority for declaring war and sending the TAF to foreign countries and giving permission for foreign armed forces to come to Turkey belongs solely to the TGNA.

7.3.3 Crisis "Coronavirus Precautions"

7.3.3.1 Precautions of TAF to Overcome the Challenges Exposed by the Corona Virus

The TAF has launched an initiative to overcome the challenges posed by the COVID-19 virus based on the motto "Training for Success, Measure for Health". Those measures aim to maintain the efficiency of ongoing operations abroad, to ensure border security and to sustain other activities such as training and counter-terrorism by eliminating the negative effects of COVID-19.

The National Defence University and its dependents such as War Institute, War Colleges and NCO Colleges have cancelled their education until August 1st, 2020.

Ceremonies, conferences, meetings, courses, fairs and seminars have also been cancelled.

The visiting activities of outsiders are also banned in the military units, headquarters, and institutions.

Officers' clubs and other military accommodation facilities do not allow people in except for compulsory cases.

The national and international exercises have been postponed. Military personnel have been put in quarantine when they return from abroad.

Call and discharge of soldiers in the conscript system has been rearranged.

COVID-19 tests are periodically made in military units and centres. Medical people in military units have been reinforced.

For daily activities, it is a must to use masks and maintain social distancing. Disinfection measures are frequently applied while using weapons or other tools in military activities.

The Turkish Air Force has aided some NATO countries with medical supplies and essential apparatus to struggle with COVİD-19 using A-400 transportation aircrafts.

The Turkish Command of Health has started another project to restructure medical facilities and research centres.

7.3.4 Interdepartmental Cooperation

The National Security Council was founded in 1983 in accordance with Article 118 of the 1982 Constitution. It consists of the President of the Republic, the Prime Minister, the Chief of the General Staff, Deputy Prime Ministers, the Minister of Justice, the Minister of National Defence, the Minister of the Interior, the Minister of Foreign Affairs, the Commanders of Land, Naval and Air Forces, and the General Commander of the Gendarmerie. The President is the head of the Council. The National Security Council delivers advisory opinions to the Council of Ministers on the designation, establishment and implementation of the national security policy and provides the necessary coordination. According to Article 117 of the 1982 Constitution, the Council of Ministers is responsible before the Turkish Grand National Assembly for ensuring security and training and preparing the Turkish Armed Forces to the protect the country. The National Security Council meets every two months. When necessary, it can meet on the proposal of the Prime Minister or with a call from the President of the Republic. The General Secretary of the Council can attend the meetings but cannot vote.

7.3.4.1 The Turkish Armed Forces

Turkey has the second largest army in NATO after the US. As one of the eight member countries in which mandatory military service exists, the greater part of the army consists of conscripts. Turkey's military manpower is estimated at 514,000 (Ref. [8], p. 363). All males between the ages of 19 and 41 are obliged to do 15 months of military service. University graduates do their military service for 12 months as reserve officers or for 6 months as privates. Turkey announced a motivated military modernization program in 1996. It aimed at acquiring high-technology equipment, upgrading older systems, producing home-grown military equipment and becoming increasingly self-sufficient in terms of military technologies [33].

7.3.4.2 Land Forces

The land forces have 402,000 active personnel. It is the second largest army in NATO and the fifth largest in the world. The structure of the land forces consists of 9 Army Corps, 1 Infantry Division, 2 Mechanized Infantry Divisions, 1 Armoured Division, 1 Training Division, 11 Infantry/Motorized Brigades, 16 Mechanized Infantry Brigades, 9 Armoured Brigades, 5 Commando Brigades, 1 Army Aviation Brigade, 2 Artillery Brigades, 5 Training Brigades and a Humanitarian Aid Brigade [10]. These units are organized as four Field Armies, a Logistics Command and a Training and Doctrine Command.

7.3.4.3 Gendarmerie

The Gendarmerie General Command is responsible for the maintenance of safety and public order. It is subordinated to the General Staff in matters related to training and education in connection with the Armed Forces, and to the Ministry of Interior in matters related to the performance of the safety and public order

duties. However, the General Commander of Gendarmerie is responsible to the Ministry of Interior. The area of duty and responsibility of the Gendarmerie covers mostly rural zones outside the Police duty zone, which comprise 92% of the total area of Turkey [23]. The Gendarmerie is responsible for maintaining safety and public order in these zones.

7.3.4.4 Naval Forces

In 2008, the naval forces had 48,600 active personnel ([22], pp. 25-26). The Navy consists of 13 Submarines, 18 Frigates, 6 Corvettes, 20 Mine Sweepers/Hunters and 24 Assault Boats. These come under the Fleet Command, the Northern Sea Area Command, the Southern Sea Area Command and the Naval Training and Education Command. Moreover, an Amphibious Marines Brigade, several commando detachments and two special operations forces (the Underwater Attack and Underwater Defence) are maintained as Marines and Special Operations Units.

7.3.4.5 Coast Guard

The Turkish Coast Guard Command is responsible for enforcing national and international laws and ensuring the safety of life and property within its area of maritime jurisdiction. Like the Gendarmerie, it is responsible to the Ministry of the Interior during times of peace.

7.3.4.6 Air Forces

The Air Force consisted of 60,100 active personnel in 2008 ([22], pp. 25-26). In terms of its structure, the Turkish Air Force consists of 17 Combat Squadrons, 1 Reconnaissance Squadron, 1 Tanker Squadron, 5 Transportation Squadrons, 3 Search and Rescue Squadrons and 10 Training Squadrons. These units are organized as two Air Force Commands: the Air Training Command and the Air Logistics Command. By April 2011, the Turkish Air Forces had 1,049 aircrafts. This fleet size ranks second in NATO after the US Air Force. The Turkish Air Force also has the highest number of F-16 jet fighters after the USA. The Turkish Air Force fighter jets can participate in international operations and exercises on all continents of the world and have long-range in-flight refuelling capability.

7.3.4.7 Ministry of the Interior and the Police

The Ministry of the Interior is responsible for internal security, public peace and the organization of civil protection. The National Police, the General Directorate of Civil Defence, the General Command of the Gendarmerie and the Coast Guard are under the jurisdiction of the Ministry of Interior in times of peace. The National Police force is organized as a Central Directorate and 81 Local Directorates, one in every province. The total number of personnel of the Turkish National Police was 229,965 as of 2010. Only two years previously it had been under 210,000 and it is expected to reach 250,000 in a few years.

7.3.4.8 Changes Following the 15 July Coup Attempt in 2016

The chain of command at the top has been changed. The chief of defence will now be appointed directly by the President, and the General Staff will be attached to the Ministry of National Defence instead of the defunct Prime Minister's Office. In addition, the President will be able to give orders directly to the commanders of Turkey's land, air, and sea forces without having to go through any other office or authority. The Supreme Military Council (YAS) has also been relieved of many of its previous functions, leaving all major decisions concerning the armed forces, including promotions and assignments of colonels and generals, to the president [13]. Furthermore, a new Board of Security and Foreign Policy, one of nine consultative bodies attached to the presidency, has largely taken over the policy guidance functions of the previously so powerful NSC.

In his new and enhanced role, the Minister of National Defence will now be a key decision-maker regarding military affairs. The defence ministry will be responsible for the education, finances, and budget of the armed forces, as well as Turkey's defence industry, shipyards, military health services and infrastructure.

In addition, the military educational system has undergone major changes. Military high schools have already been closed, and the existing military academies have been fused into a new National Defence University under the Ministry of National Defence. The TSK has also been stripped of many of its former units and functions. Most importantly, the paramilitary gendarmerie and the coast guard have been fully subjected to the Ministry of Interior.

Moreover, the establishment of a new National Defence University will discontinue the position of Turkish military academies – institutions with traditions that go back over a century.

In recent decades, both police and gendarmerie forces have certain roles contributing to international security. For instance, the Turkish police units have been tasked in Bosnia and Herzegovina and Kosovo to support the education of local units within international arrangements [25]. Moreover, the Turkish Gendarmerie has been tasked with educating local forces in countries such as Gambia and Nigeria.

In reference to existing doctrinal documents:

- At the Ministerial level, Directives and Guidance of National Defence Ministry.
- At the level of Turkish General Staff, Document of National Military Strategy.
- At the level of the Forces (Land, Marine and Air Forces), each force has its own doctrine, concept and strategy documents.

To develop doctrines and concepts, Army Training and Doctrine Command was established in the 1990s, similar to the US TRADOC. Within this unit, there are components such as war simulation centres and the Centre for Lessons Learned.

7.3.4.9 The Civil-Military Cooperation Legislation and Regulations

Comprehensive and various administrative and legal instruments exist in Turkey authorizing the national authorities to carry out activities related to civilian state of emergency in crises and war as well as peacetime and to constitute an effective mechanism in these areas. The important national legislation and regulations within this framework are stated below [2]:

- Law and Regulations on Mobilization and State of War;
- Directive on Mobilization and Preparations for War;
- Law on National Preservation;
- Law on the National Defence Obligation;
- Emergency State Law and regulations, instructions based on this law;
- National Security Council and the General Secretariat of the National Security Council Law and Regulations;
- Civilian Defence Law;
- Law Related to How to Perform Transport and Communications Services in States of Emergency and War;
- National Alarm System Circular;

- Prime Ministry Crisis Management Centre Regulations;
- Law Related to the Measures to be Taken and Aid to be Given Due to Disasters that Influence Public Life;
- Provincial Administration Law;
- Martial Law;
- Law for Protection Against Overflowing Rivers and Floods;
- Regulations Related to the Principles of Emergency Aid and Planning Related to Disasters;
- Circular Related to NATO Civilian State of Emergency Planning Activities; and
- Law and Regulations related to War Industry Activities.

The civilian state of emergency legislation mentioned above also regulates civil-military cooperation subjects besides the civilian state of emergency activities to be carried out in periods of peace, crisis and war. A decree in the legislation also specifies the necessity of coordination based on cooperation between civilian and military authorities [17].

The Turkish crisis management system has been renewed in recent years based on the Constitutional changes at both top civilian and military levels. Changing the nature of the decision making system from the prime ministry to the presidency, the President and his offices has been the focal point of the whole crisis management [11]. However, each branch of state from the level of ministries to city level has its own crisis management organization coordinating both civilian and military efforts. Those organizations from top to bottom have functioning existing and renewed acts, arrangements, or protocols.

Crisis management is activated in peace time with a nucleus and based on the escalation of the crisis, the preparedness and manpower of crisis management centres are reinforced.

Crisis response planning and operations at the international level have two categories;

1) To respond to international political or military crisis; and
2) To prevent or mitigate the effects of natural disasters.

Civil-Military cooperation in Turkey is established to ensure the following targets [1]:

- To continue the functions of the government in times of crisis and war;
- To perpetuate the social and economic life;
- To provide for the protection of the people against the threats and risks stemming from war and disasters;
- To facilitate reconstruction after attacks;
- To contribute to the continuing efforts of the NATO/European-Atlantic Partnership Council (EAPC) at an international level; and
- To provide for the rehabilitation of disaster regions.

7.3.4.10 Areas of Activity

In the aftermath of natural disasters such as earthquakes, floods, avalanches, landslides and large fires, the civilian sector will be supported by the military sector. In case of mobilization or war, the military sector will be supported by the civilian sector. At times of crisis and war, all kinds of communications and transport equipment belonging to the public and private organizations can be given over to the operations control of the Turkish Armed Forces (TAF), with a decision of the Council of Ministers, if necessary.

This cooperation between the civilian and military sectors includes various fields extending from local to central authority. The civilian-military fields of cooperation in Turkey are given below (Ref. [35], p.112):

- The preparation of plans, procedures and principles related to mobilization and preparation for war;
- The determination of priorities in the planning of the national resources related to the needs of the Armed Forces, public and private sectors and the people;
- The utilization of civilian and military resources and services, such as food, agriculture, industry, energy, transport, communications, health and manpower;
- The support of military preparations and operations;
- The implementation of necessary measures against an enemy attack or a disaster where civil defence is concerned, such as protection of the people including the areas of warning, determining and alarm, population movements, search and rescue, medical services, temporary shelter and the distribution of basic necessities such as food and clothing;
- The identification of vulnerable regions or facilities that might be subject to enemy threats, including security regions and military restricted and security zones;
- The taking of necessary measures related to various security concerns and internal turmoil;
- The making of necessary arrangements for providing the public with information on training and exercises; and
- The coordination of civil-military cooperation and NATO Civil Emergency Planning.

7.3.5 International Interoperability

Logistics interoperability in the international arena is achieved within two processes;

1) In NATO operations, Agreements on the force level requirements from the nations and supply chain arrangements as foreseen in the logistics plans in line with Memorandum of Understanding (MOUs) and Host Nation Support (HNS) agreements.
2) In Non-NATO operations such as multinational coalitions, it is synchronized in accordance with theatre level arrangements like the lead nation concept or based on demands from nations.

7.3.6 Roles and Responsibilities of Different Stakeholders

In addition to the capacities of the Ministries of Foreign Affairs, National Defence, Interior and Justice to make precautionary recommendations on matters related to identifying domestic and external threats, monitoring alliances, the TAF, and internal security, the role of the Directorate General of Migration Management, founded under the Interior Ministry, is expected to grow.

Civil society organizations are motivated, encouraged, and financed to draft objective and scientific research reports as well as studies in their respective fields of specialty [26].

With the analyses that it presents to the Ministry of Foreign Affairs as the main actor, along with its ability to keep diplomatic channels open, the National Intelligence Organization (NIO) swiftly mobilizes the decision-making mechanisms of the state.

Important amendments were introduced to Law No. 2937 on the State Intelligence Services and National Intelligence Organization with the law dated April 26, 2014.

7.3.7 Standing Legal Provisions for Activation of the System and Further Escalation

According to Turkish Constitution Article 117, the cabinet has the main responsibility to ensure national security. Article 118 states that the National Security Council can make proposals to the cabinet on security issues. Following the transition to the presidential system, the president has been the top man for decision making, being the chief of cabinet as well.

Based on the crisis management system from top to bottom, within the decisions of cabinet, crisis management centres are reinforced by both civilians and military people. The crisis management system (CMS) has its own standard operating directives at each level and is supported as required by infrastructure and communication systems. CMS works in shifts and is exercised regularly in peacetime.

Stakeholders of the system:

- The cabinet members from each ministry including foreign relations, national defence, transportation and communication, and health;
- Military people based on their expertise;
- Members of the intelligence services;
- Civilian agencies such as TİKA (to support the local infrastructure), Kizilay (NGO for the recovery of civilian victims), AFAD (recovery in natural disasters), civilian defence units for war time; and
- Governors and mayors at local levels.

In Turkey's surrounding geography, which is beset by peripheral risks, threats, and instabilities, it is critical that the TSK improves its capacity for flexible deployment and operational leveraging (mobility, flexibility, usability, firepower projection, sustainable operation).

Growing instability on its borders, illegal movement of peoples, mass migrations, drugs and arms trafficking, and Turkey's location along land and maritime transit routes further expand the duties and responsibilities of the Ministry of Interior. Moreover, the ongoing uncertainty regarding maritime jurisdiction in the Aegean and the Eastern Mediterranean, as well as illegal migration attempts further increase the responsibility and importance of the Coast Guard Command in these regions.

Concerning recent discussions about restructuring the Gendarmerie General Command, it is crucial that the institution's apolitical position is preserved and that its duties and authority over border and domestic security are compatible with the realities of national and regional security (Ref. [30], p.46). Another vital institution for the country's security, the Turkish National Police should promptly distance itself from the current environment of controversy. In terms of its duty, authority, and equipment inventory, it should not overlap with the TSK and the Gendarmerie General Command.

7.4 CHALLENGES OF IMPLEMENTATION

7.4.1 Joint Planning, Training, and Procurement

The Turkish Armed Forces (TAF) has the objective of making contributions to regional and world peace and stability. The TAF, with the awareness that it has "To Be Always Ready for War" to preserve and develop peace and stability, gives importance to training and exercises. Training in the TAF is planned and performed by taking into consideration the experiences acquired in the operations carried out in the past, probable areas of utilization of the TAF, joint training requirements in the scope of NATO and the various risk factors in the region.

The TAF is an institution that strives to modernize and prepare its structure and personnel for the future. In this context, the TSK implements training programs and plans that correspond with contemporary systems. Hence, it possesses the accumulation of knowledge and experience as well as the staff and organizational structure to ensure peace and stability in its region.

The TAF Training system has a structure parallel to the Turkish National Education System and Turkish Higher Education System. The TAF training-education system was established with the objective of having the officers, non-commissioned officers, civil servants, sergeants, corporals and privates acquire necessary capabilities for performing the duties given to the TAF by the constitution and laws.

The training and education system of the TAF is a whole composed of two subsystems built on the trio of Training Centre-School-Unit, which complement each other.

These subsystems are:

- Individual training comprising the training of officers, non-commissioned officers, civil servants, specialist gendarmes, specialist sergeants, corporals and regular sergeants, corporals and privates, and
- Unit training preparing the units for combat.

Joint planning is achieved through coordination and exercises of operation plans prepared by the civilian and military cells. Based on the outputs of those exercises, the interoperability and procurement requirements are foreseen to include strategic force and capability targets. Ministries such as Internal Affairs or National Defence have their own budget and procurement system for emergency, mid-term or long term periods.

Training and exercise planning issues are also in the hands of the state system. Training institutions such as the National Defence University, Academy of National Security, and NATO Excellency Centres have curriculums including crisis management, planning, interagency coordination issues.

SSM has a large say in defence procurement projects, as it can accept or reject proposals, choose to evaluate them or ignore them, request new proposals, or cancel the tender, without incurring any responsibilities. The National Defence Executive Committee can choose to award the Project to any contractor candidate.

Current weapons procurement has the following legal distribution of functions: the Council of Ministers decides the general strategy, the Defence Industry High Coordination Board is responsible for guiding directives, the Defence Industry Executive Committee is responsible for final decision making, the General Staff is the requirement generator, and SSM is responsible for procurement and development of the domestic defence industry (Ref. [19], p. 31).

Turkey's National Military Strategy (TNMS) and the Planning and Programming Directive (PPD) are used as a source in the determination of the Defence Industry Strategy. Coordination is made with the Ministry of Foreign Affairs as regards carrying out the Defence Industry Strategy in conformity with foreign policies and in compliance with the international agreements to which Turkey is a party [5]. The Ministry of National Defence is the coordinating authority in the implementation of this strategy.

Turkish defence policies and armed forces' operations, capabilities and expenses cannot be considered separately from civil-military relations.

Through the military modernization and defence industrialization programs, Turkey has been able to produce new age military equipment.

According to the 2017 – 2021 Strategic Plan of the UDI, some of the ongoing projects include the development of air and ballistic missile defence systems, the TF-X fighter jet, Anti-Air Warfare (AAW) defence frigate, and submarines with air-independent propulsion systems [29]. As a result of procurement efforts, TAF ranks among the top militaries of the world in terms of some of its equipment and systems. For instance, Turkey is one of the 15 countries in the world that has Military Information, Surveillance, and Reconnaissance (ISR) Satellites. The Turkish Air Force has 1,018 aircrafts, and among NATO countries, Turkey's total fleet size is outranked only by the USA [20]. Additionally, Turkey is among the top 10 countries worldwide in terms of the number of MBTs in active service.

7.4.2 Standing Operating Procedures and Equipment Compatibility/Interoperability

Standing Operating Procedures (SOPs) comprise the tasks and coordination methods of different agencies. Those procedures and related equipment such as communication and transportation are employed in crisis management exercises either physically or in simulation centres. Those exercises are achieved through scenarios within the related operation plans or the crisis management plans. Equipment interoperability in international operations has been studied and experienced in recent NATO or international coalition operations. The Turkish procurement system refers to the interoperability criteria while supplying new capabilities. For unforeseen conditions, local solutions are achieved through new or temporary supplies (sometimes to reinforce the other side) based on the protocols.

SOPs and/or protocols among the different agencies also include the coordination of matters such as fuel standards, power plugs and sockets, radios using the same frequency.

7.5 FUTURE DEVELOPMENTS AND ONGOING DISCUSSIONS

Turkey has a volatile geostrategic environment which exposes it to many contingencies for being prepared. Particularly the Middle East situation has required Turkish intervention into Syria and Libya. Turkey has also been busy with transnational separatist terrorism for a long time. In addition, Turkey has had some disputes with neighbour countries regarding the sovereignty of some territories or marine areas. This busy security agenda has required Turkey's armed forces to stand by ready and dynamic for more than one contingency simultaneously.

Turkish interventions have ensured an army constantly learning, experienced and innovative to bring local solutions in different theatres. In addition to Lesson Learned Centres and Battle Simulation Centres in Army Doctrine Command, universities and civilian research or think-tank centres are periodically issued journals to cover the specific aspects of operations and public opinion [4].

As preliminary conclusions, we may assess the following:

1) Turkey has a well-working crisis management system on both civilian and military sides. There are established documents to task and coordinate the stakeholders and ensure interoperability in national and international contingencies.
2) Recent interventions have taught Turkey to develop her solutions at each theatre and maintain self-adequacy in technology for innovations.
3) The complexity of theatres with proxies and many nations with different interests, have forced to Turkey to change her partners based on conjuncture in different phases of contingencies.
4) As a lesson learned from multinational operations, the nations should have a firm commitment to ensure their mutual interests. Otherwise, reluctant contribution and divided interests cause inefficiency in operations.

5) Last but not least, Turkey has learned that future crisis requires that agreements be made with stakeholders at the beginning especially regarding migration issues such as quotas, commitments, humanitarian aid.

7.6 REFERENCES

[1] Akay, H. (2009), "Türk silahlı kuvvetleri: Kurumsal ve askeri boyut", In A.Bayramoğlu, and A. İnsel (Eds.), Almanak Türkiye: 2006 – 2008 Güvenlik Sektörü ve Demokratik Gözetim, Tesev, pp. 117-171.

[2] Aknur, M. (2013). "Civil-military relations during the AK-Party era: Major developments and challenges", Insight Turkey, 15(4), pp. 131-150.

[3] Aktas, T. (13 October 2016), "Details emerge of Turkish military base in Somalia", Anadolu Agency. Archived from the original on 7 March 2017, Retrieved 7 March 2017.

[4] Aydinli, E. (2009), "A paradigmatic shift for the Turkish generals and an end to the coup era in Turkey", Middle East Journal, 63(4), pp. 581-596. DOI: https://doi.org/10.3751/63.4.13

[5] Beriş, H.E. (2012), "Dünyada ve Türkiye'de savunma harcamalarının demokratik denetimi", SDE Analizi: Ankara.

[6] Bilgin, P. (2005), "Turkey's changing security discourses: The challenge of globalisation", European Journal of Political Research, Vol. 44, No. 1, pp. 175-201.

[7] Cizre, U. (Ed.) (September 2006), Almanac Turkey 2005, Security Sector and Democratic Oversight, TESEV, Istanbu,.

[8] Demirtaş, B. (2012), "Understanding Turkish perception of conscription and reluctance to reform: A Westphalian approach in a Post-Westphalian world?", Iran and the Caucasus 16, pp. 355-368.

[9] Dervişoğlu, S., and Köksal, S. "Turkey in a Changing Global and Regional Security: Analysis and Recommendations", Global Relations Forum Task Force Report, (İstanbul, Feb 2015), p. 13.

[10] Global Firepower.com, "2017 Turkey military strength", Accessed 15 August 2017, http://www.globalfirepower.com/country-military-strength-detail.asp?country_id=turkey

[11] Göcek, F.M. (2011), "The transformation of Turkey: Redefining state and society from the Ottoman Empire to the Modern Era," London, I.B. Tauris.

[12] Gülden, A., and Gunluk-Senesen, G. (2016), "Turkey's changing security perceptions and expenditures in 2000s: Substitutes of complement?" The Economics of Peace and Security Journal 11, no.1, p.35.

[13] Gürcan, M. (16 September 2016), "How post-coup purges depleted Turkey's military", Al-Monitor, http://www.almonitor.com/pulse/originals/2016/09/turkey-military-needs-two-year-fill-ranks-emptied-by-purge.html

[14] Gürpınar, B. (2013), "Milli Güvenlik Kurulu ve Dış Politika", Uluslararası İlişkiler 10, No.39, p.73.

[15] Gürsoy, Y. (2017), "Between military rule and democracy: Regime consolidation in Greece, Turkey, and beyond", Ann Arbor: University of Michigan Press.

[16] Gürsoy, Y. (2017), "Turkish defence policies and armed forces: Continuities and changes since the Cold War", Aston University, EPCR General Conference, pp. 22-23.

[17] Haugom, L. (2019), "The Turkish Armed Forces and civil-military relations in Turkey after the 15 July 2016 coup attempt", Scandinavian Journal of Military Studies, 2(1), pp. 1-8. DOI: 10.31374/sjms.14.

[18] Jacinto, L. (13 July 2020), "Turkey's post-coup purge and Erdogan's private army", Foreign Policy, http://foreignpolicy.com/2017/07/13/turkeys-post-coup-purge-and-erdogans-private-army-sadat-perincek-gulen/amp/

[19] Karahan, Y. (2014), "Supervision of defense procurement in Turkey", [Türkiye'de savunma harcamalarının denetimi], PhD Thesis, Adnan Menderes University.

[20] Kasapğlu, C. (15 May 2020), "Turkey's growing military expeditionary posture", Terrorism Monitor, 18(10).

[21] Kızmaz, E. (September 2007), "Turkish defense industry and undersecretariat for defense industries", Master's Thesis, Department of International Relations, Bilkent University, Ankara.

[22] Library of Congress – Federal Research Division. Country Profile: Turkey, (August 2008).

[23] McGregor, A. (25 November 2008), "Turkey's gendarmerie", Terrorism Monitor, Jamestown Foundation, 6(22), p.32.

[24] McGregor, A. (June 2008), "Arming for asymmetric warfare: Turkey's arms industry in the 21st Century", Jamestown Foundation.

[25] Oğuzlu T., and Güngör, U. (2006), "Peace operations and the transformation of Turkey's security policy", Contemporary Security Policy 27(3), pp. 472-488.

[26] Özpek, B.B. (2014), "Pseudo-transformation of civil-military relations in Turkey", (Analysis No. 267), Retrieved from Italian Institute for International Political Studies: https://www.ispionline.it/en/pubblicazione/pseudo-transformation-civil-military-relations-turkey-10845

[27] Sarigil, Z. (2011), "Civil-military relations beyond dichotomy", Turkish Studies, 12(2), pp. 265-78. DOI: https://doi.org/10.1080/14683849.2011.572633

[28] Secretariat General of the National Security Council, www.mgk.gov.tr Retrieved 18 May 2019.

[29] Stockholm International Peace Research Institute (SIPRI), "Data for all countries", SIPRI Military Expenditure Database, https://www.sipri.org/databases/milex Accessed 15 August 2017.

[30] Sünnetçi, I. (April 2009), "The Turkish defense industry: Dramatic transformation under the guidance of SSM," Military Technology, April 2009, pp. 93-106.

[31] The White Paper, "The national defense policy and strategy of Turkey", (2013). Türkiye'nin Savunma Politikası ve Askeri Stratejisi, Beyaz Kitap Kitap, Dördüncü Bölüm, http://www.msb.gov.tr/Birimler/GnPPD/GnPPD BeyazKitap.htm, Ankara, Retrieved 10 January 2014.

[32] Torumtay, N. (2009), "Turkey's military doctrine", Dış Politika 1.

[33] Turkish Armed Forces, “TSK official history information”, Archived from the original on 29 June 2013, Retrieved 2 January 2014.

[34] Turkish Ministry of National Defence, www.msb.gov.tr Retrieved April 2017.

[35] Yılmaz, S. (2009), “Ulusal savunma: Strateji, teknoloji, savaş”, Kum Saati Yayınevi, Istanbul.

Chapter 8 – A COMPREHENSIVE NATIONAL DEFENCE SYSTEM: A UK PERSPECTIVE

Andrew Houston
DCDC, Defence Academy
UNITED KINGDOM

8.1 INTRODUCTION

The purpose of this case study is to describe the UK's approach to civil-military cooperation within the evolving framework of Comprehensive National Defence. Civil-military cooperation has a long history but varies from country to country. The UK does not maintain an established force that is specifically tasked with supporting homeland security in a similar vein to the Gendarmerie in France or Carabinieri in Italy, nor does it have the framework or resources to adopt a similar model to the National Guard in the US. In most threat scenarios there is a civilian department lead with the military in a supporting role. The Royal Navy and Royal Air Force have specific responsibilities for the integrity of territorial waters and UK airspace respectively, but the British army has no such role in domestic security. Whilst there are operations that dictate readiness levels in response to terrorist threats it is important to highlight that the purpose behind these activities is to provide a mechanism whereby police capacity is made available through more mundane security tasks being fulfilled by army units. It is not about deploying troops on the streets to directly deal with a terrorist threat. This remains the responsibility of the police, or in a worst-case scenario, special forces. It is important to highlight the UK's unique approach up front to understand how it approaches National Defence and how primacy is the central issue over how military forces are employed in a domestic setting within the UK.

National Defence is undoubtedly far broader than just the military and attention should be paid to the emergency services, the security services and numerous government departments that have stakes in critical national infrastructure. However, this case study maintains a deliberate bias towards the military contribution and does not attempt to provide an analysis of other contributors. Specific detail over how each of the Armed Services contributes to National Defence is beyond the remit of this case study due to classification and scope. Instead, an overview of how the UK Defence community as a collective carries out its contribution to domestic security tasks will be presented and analysed against the context of a Comprehensive National Defence System in the current threat environment. The key document that will be used throughout this case study is JDP 02, *UK Operations: The Defence Contribution to Resilience and Security* (3rd edition) [6]. Specific areas that require specialist input such as logistical interoperability and onward staging of forces under NATO obligations are not included.

The case study is structured into three separate parts. The first part analyses threat perception within the UK referring to national objectives and priorities and includes an analysis of what is meant by the term Comprehensive National Defence through a UK lens. Key ideas from the Integrated Operating Concept 2025 [7] will be presented to highlight the new threat landscape the UK faces. The second part of the case study articulates the current Defence contribution to resilience and security, and where appropriate, how new methods must be identified to meet the new challenges the UK faces. The third and final part to this case study will discuss the implementation challenges to achieve a Comprehensive National Defence System from a UK perspective before highlighting preliminary conclusions.

8.2 PART 1: FRAMING THE CHALLENGE

To best analyse threat perception, the first task is to refer to existing documentation that articulates identified threats and associated challenges across the spectrum. In this case study, the documentation in question

is taken from the latest security reviews. The relationship between identified threats and National Security Objectives is then discussed against the idea of a Comprehensive National Defence System highlighting the frictions unique to the British approach.

8.2.1 Understanding the Threat

The pace of technological change across the world is rapid and brings with it a host of challenges. Some of these are familiar, but perhaps more importantly, technological change brings with it a range of new threats to which our response remains uncertain. The National Security Capability Review (NSCR) from March 2018 places emphasis on the continuing trend of long-term shifts in the balance of economic and military power, and the increasing competition between states as well as the challenge posed by non-state actors (Ref. [2], p. 5). As threats become more complex and intertwined in an uncertain and volatile world it is important to articulate and understand the security environment to be able to recognise where vulnerabilities exist. Against this context, the NSCR builds on the challenges that were originally highlighted in the Strategic Defence and Security Review (SDSR) 2015 and outlines 6 dominant challenges (Ref. [2], p. 5) for the UK over the next decade:

- The increasing threat posed by terrorism, extremism and instability;
- The resurgence of state-based threats; and intensifying wider state competition;
- The erosion of the rules-based international order, making it harder to build consensus and tackle global threats;
- The impact of technology, especially cyber threats and wider technological developments;
- The ongoing growth in serious and organised crime and its impact; and
- Diseases and natural hazards affecting the UK.

The NSCR is effective in highlighting how important these security challenges are against significant changes since SDSR 2015, not least the UK's decision to leave the EU. As 'Global Britain'[1] (Ref. [2], p. 30) articulates how the UK sees itself in the world, the framework that was laid out in the SDSR 2015 to represent the breadth of British national security interests remains valid and sets the UK's three National Security Objectives (NSOs) (Ref. [2], p. 9):

1) National Security Objective 1 is to **protect our people** – at home, in our Overseas Territories and abroad, and to protect our territory, economic security, infrastructure and way of life.
2) National Security Objective 2 is to **project our global influence** – reducing the likelihood of threats materialising and affecting the UK, our interests, and those of our allies and partners.
3) National Security Objective 3 is to **promote our prosperity** – seizing opportunities, working innovatively, and supporting UK industry.

Viewed together the NSOs clearly state the strategic interests of the UK and the six key challenges identified in the NSCR can be thread across all three NSOs. There are numerous well-informed publications within the Ministry of Defence and HM Government that highlight the key challenges and trends that are likely to affect the nation. The NSCR is a good reference point but Global Strategic Trends serves as a useful document to frame the full range of future strategic challenges [8].

However, the extent to which threats are perceived by UK society is less clear. It may seem an obvious point that security professionals within government and Defence are able to articulate current threats and which are

[1] As Global Britain, we are reinvesting in our relationships around the world. We are championing the rules-based system, which has served our interests as a global trading nation and is of vital importance as geopolitics becomes more contested. And we are using our soft power to project our values and advance UK interests.

most dangerous to the nation but national security, and those who contribute to it, is perhaps less well understood by the public. This is supported by the findings from the MOD annual poll in 2017 that found despite 68% of respondents believing the role of the army is defending the state, only 11% responded that this included supporting the police in a national emergency, with just 6% believing the army plays a role in countering terrorism (Ref. [1], p.3). This provides stark evidence that the proposition made by Keith Jeffrey in 1985, that 'the British army, when it fights, fights abroad' (Ref. [3], p. 51) still has resonance today in how the British military are perceived by the public they serve. Therefore, the contribution from the military to a Comprehensive National Defence System through a UK lens is limited. Rather, a Comprehensive National Defence is more focused on a civilian lead with the military adopting a limited supporting role. JDP 02 captures this sentiment in detail which will be explored more thoroughly later in the case study.

8.2.2 An Approach to National Defence

The term Comprehensive National Defence System is not one that is used in the UK and yet it is important for the purposes of this case study to analyse what is meant by it. NSO 1, protect our people, is arguably at the heart of what a Comprehensive National Defence System should be about, extending territorial security to include economic security, protection of infrastructure and the British 'way of life' but the UK has frequently sought to project its influence abroad and 'defend away'.

Indeed, by virtue of its name one would be forgiven for thinking the Comprehensive Approach from 2010 must have included an element of National Defence but in reality, it concerned the Ministry Of Defence (MOD), the Foreign and Commonwealth Office (FCO) and the Department of International Development (DFID); essentially outward looking departments (Ref. [11], p.72). The UK Comprehensive Approach has since faded into obscurity and no longer has relevance to current policy. The Integrated Approach and Full Spectrum Approach followed and were attempts to improve the ways in which different departments within the British governments worked together but neither lasted [4]. The Fusion Doctrine referenced in the NSCR is the latest evolution and arguably addresses National Defence more directly than the Comprehensive Approach ever did through a far broader remit and more focused coordination across the full breadth of government departments and ministries. Figure 8-1 captures the totality of Fusion Doctrine and provides a pictorial insight into how multiple levers of national power are cohered toward the interconnected NSOs.

Without going into overbearing detail, the key takeaway from the Fusion Doctrine for this case study is its name, whereby it has deliberately been given a more assertive title with the use of *doctrine* rather than *approach.* The subtle change reflects a more mandatory application across government rather than a vague encouragement to adopt new behaviours. However, whether this translates towards a Comprehensive National Defence System is less certain, especially given the public's relatively poor grasp of national security but the conceptual underpinning is moving in the right direction.

The British public's relatively poor perception of national security does not reflect a limited capacity to grasp threats and associated challenges. Instead, it highlights the lack of engagement between the British government and the British people on matters of Defence policy (Ref. [5], p. 27). The apparent communication gap undermines the ability to effectively develop a coherent strategy for the use of military force and acts as a barrier to address how the military can better contribute to National Defence in a domestic setting. Not only is the public removed from most discussion surrounding Defence but according to one commentator, the Whitehall mindset towards the public on matters of Defence policy tends to be one of distrust and suspicion which renders it incapable of responding coherently to the changing character of conflict (Ref. [5], p. i). Given the acknowledgement in numerous documents that threats are evolving and becoming more complex and intertwined, it is vital that efforts that contribute towards a more effective Comprehensive National Defence System are made. Indeed, the impact of COVID-19 is still not fully understood but it nonetheless provides a stark reminder on the importance of how Defence must be able to work across the breadth of government and not just across Defence and Security departments (Ref. [9], p.3). The Fusion Doctrine is still maturing but aims to deliver this foundation through better integration.

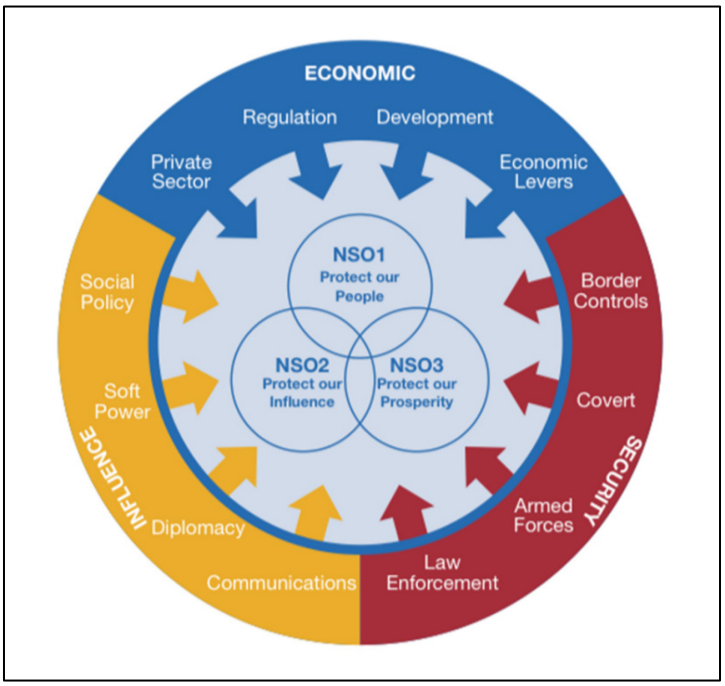

Figure 8-1: UK Fusion Doctrine (Ref. [2], p. 10).

8.2.3 Towards a New Integrated Operating Concept

This chapter has already given recognition to the complexity of the current threat environment and how the world is increasingly more competitive and volatile with both state and non-state actors seeking advantage where they can. The Information Age is upon us and ideas based in the Industrial Age are becoming less applicable to our modern reality. This is articulated within the UK's new capstone operating concept as the era of persistent competition in which long-held assumptions are frequently challenged (Ref. [7], p. 1) Distinctions between war and peace, at home and abroad, state and non-state, virtual and reality are less clear, and the rules-based international order is increasingly tested.

An expeditionary mindset whereby the homeland is kept safe by challenging enemies at reach is no longer feasible. Threats are diversifying and becoming more sophisticated to bypass traditional Western strengths and the array of capabilities available to adversaries is growing. The Integrated Operating Concept 2025 provides the basis to the UK's understanding of the current threat environment and has significant implications for how Defence can better contribute to national security and by extension, a Comprehensive National Defence System. It represents a potential shift in focus and recognition of the importance of homeland resilience.

8.2.4 Part 1 Summary

To summarise the key points from Part 1 it is clear that the UK approach to National Defence and how it is organised is predominantly expeditionary in nature which causes frictions in attempting to apply a Comprehensive National Defence System approach to existing force structures. However, Fusion Doctrine offers a model to bring coherence across the multiple stakeholders involved in National Defence. Through better coordination between government departments involving the full range of national levers of power, Fusion Doctrine aims to deliver enhanced integration which is a vital component of a functioning Comprehensive National Defence System. In conjunction with the latest thinking in the Integrated Operating Concept 2025, highlighting the challenges that the UK is likely to face and how the Defence can be better placed to respond to them, the conceptual foundations moving towards a Comprehensive National Defence System are growing with resilience as a core element.

8.3 PART 2: UNDERSTANDING THE REQUIREMENT

An inescapable facet of a Comprehensive National Defence System is building processes, infrastructure and capabilities that deliver resilience. Yet resilience means different things to different people and at the national level, it is complex and difficult to measure. Understanding how Defence sees resilience and how it contributes to it in a domestic setting is an important step in identifying the strengths and weaknesses of the UK approach.

8.3.1 The Defence Contribution to Resilience and Security

JDP 02, *UK Operations: The Defence Contribution to Resilience and Security* (3rd edition) outlines how Defence contributes to the nation's resilience and security, both routinely and when facing crises, as part of an integrated approach to civil contingency (Ref. [6], p. v). It replaced its previous version from 2007 and reflects the revised Military Aid to Civil Authorities (MACA) policy from 2016. It highlights upfront that there is a clear distinction between defending the UK against military threats and civil contingencies, and states that Defence of the UK is out of scope with the document focus on support to civil contingencies. MACA as an activity cannot be separated from civil contingency and is defined in JDP 02 as:

> *Military operations conducted in the UK and Crown Dependencies involving the employment of Defence resources as requested by a government department or civil authority. This is subject to Defence Ministerial approval, either prior to, or at the time of an event* (Ref. [6], p. 3).

MACA forms part of the refined civil response to resilience challenges following a series of events that hit the UK in the early 2000s. Under MACA, Defence has a supporting role providing niche capabilities, or more generalist support when the civil authorities' capacity/capability is overwhelmed by an incident, when directed to do so, or when preparing for major national events (Ref. [6], p. 4). Examples include numerous flooding events, the 2012 Olympics and 2014 NATO Summit. COVID-19 can also be added to the list. It is useful at this point to highlight the definition to resilience, as used by the Cabinet Office:

> *The ability of the community, services, [geographical] areas or infrastructure to detect, prevent, and if necessary, to withstand, handle and recover from disruptive challenges* (Ref. [6], p. 3).

It is clear from this definition that resilience is focused on the local level and that through the use of 'if necessary', a supporting contribution is made. The tone with which this definition is applied throughout JDP 02 sees disruptive challenges as events that are a result of natural hazards, major accidents, or terrorist activity. Although contingency planning is inevitable, the model from a Defence perspective is essentially reactive in nature and through its design, Defence does not have a proactive role and must be approached for help by other government departments.

The Civil Contingencies Act 2004 provides the framework for civil protection and categorises responders. It is important to note that Defence is not recognised as a categorised responder with the emergency services and local authorities identified as Category 1, and cooperating bodies less likely to be involved in planning work but important for responding to incidents that affect their specific sector in Category 2. The use of the military has been frequently framed as a 'last resort' option but is increasingly seen as supporting the lead government department in the most serious civil contingency challenges reflecting HM Government's integrated emergency management model based around Plan, Respond, Recover. However, it is important to recognise that the contribution to such resilience activity is usually provided by the military through spare capacity with limited forces held against domestic readiness tasks (Ref. [6], p. 40).

The provision of military assistance is governed by four principles (Ref. [6], p. 40), authorised when:

- There is a definite need to act and the tasks the Armed Forces are being asked to perform are clear;
- Other options, including mutual aid and commercial alternatives, have been discounted;

- The civil authority lacks the necessary capability to fulfil the task and it is unreasonable or prohibitively expensive to expect it to develop one; and
- The civil authority has all or some of the capability, but it may not be available immediately, or to the required scale, and the urgency of the task requires rapid external support from the MOD.

MACA is led by the Standing Joint Commander (UK) who holds primary responsibility for overseeing the Defence contribution to civil contingencies activity. The Standing Joint Commander (UK) is supported by full-time liaison officers provided by each service whose role is to ensure timely and effective liaison with other government departments and civil authorities. With few exceptions MACA is not funded from within the MOD and is paid for on a repayment basis from the request originator operating in accordance with the MACA principles outlined above.

The importance of primacy is essential to understand. In almost all scenarios concerning the defence and resilience of UK, the lead government department will not be Defence. Apart from the relatively unlikely event of a direct military threat to the UK homeland or territory, Defence takes a supporting role. However, the supporting role is based on one of reacting to a specific request. The ability to take a more proactive approach and actively offer capability to other government departments and civil agencies is limited. This is important to highlight as the notion of a Comprehensive National Defence System infers a far more active role for the military contributing to protection tasks and deterrence. This type of model has faded with the end of the Cold War and changing role of the Territorial army to becoming the army Reserve with little to no specified responsibility for domestic security tasks. JDP 02 highlights three possible legal bases for a MACA deployment:

- The Royal Prerogative for military tasks where support is supplied in addition to civil authorities' capabilities;
- A Defence Council Order (DCO) under the Emergency Powers Act 1964 for civilian tasks where support is supplied instead of civil authorities' capabilities; or
- Emergency regulations made under Part 2 of the Civil Contingencies Act 2004.

The separation of MACA from other military tasks and the legal basis behind it is noteworthy. It frames how the UK views domestic security and the limited role the military plays within it. The UK has a long history of not accepting a large standing army that dates back to the Bill of Rights in 1688 and its understanding of the place of military power in the context of its parliamentary and liberal traditions (Ref. [5], p. 2). This approach differs from some of its continental neighbours where an established force that has direct responsibilities for domestic security is maintained.

JDP 0-01, *UK Defence Doctrine* has a far wider scope and articulates how the Defence of the UK is conducted. Although its approach is implicit rather than explicit, it is useful to highlight that in giving emphasis to national interests being underpinned by a secure and resilient UK, it refers to JDP 02 as the lead document for this area. JDP 0-01 goes further to emphasise the importance of shaping a stable world and that in doing so, 'to tackle potential threats at source' (Ref. [10], p.6). Using a simplistic analysis, it is clear that the UK approach to National Defence remains to 'defend away' and by implication the bias highlighted by Jeffrey in 1985 about fighting abroad is still applicable to the British model. This represents a potential gap in doctrine where security and resilience are based almost exclusively on civil contingencies with the military in a limited supporting role and the primary focus of the military instrument concerned with deploying at reach. When revisiting the 6 challenges outlined at the start of this case study from NSCR 2018, it is clear that JDP 02 only really addresses the last challenge, one of diseases and natural hazards affecting the UK. The military contribution to the remainder is less well defined in open-source documents, which is surprising for challenges associated with technological innovation and cyber threats, and perhaps also organised crime where a coordinated response that uses a military contribution may be an effective option

to offer decision-makers tasked with securing UK interests at home. Resilience as a concept is applicable to all the identified challenges in the NSCR and yet, the British approach only seems to make a direct link to matters of civil contingencies.

The threats referenced in documents like the Integrated Operating Concept 2025 clearly convey that modern threats are no longer clearly separated into neat categories of home and away and that the distinction between war and peace is increasingly blurred. Although the UK approach to resilience and security has many strengths, it is debatable whether the current framework would be able to effectively respond to a cascade of threats or a complex challenge that absorbs more than just spare capacity from an already overstretched force. COVID-19 represents an interesting example whereby the scale of the crisis drew in a lot of additional military resource and called into question some efficiency saving approaches that include 'just-in-time' logistics and having limited redundancy to call upon at short notice. The need to identify new methods in response to 21st century challenges is clear.

8.3.2 New Challenges, New Methods

In response to new challenges that range in complexity and scale, the role of deterrence in a Comprehensive National Defence System is vital. Deterrence by its nature should encompass a comprehensive, all of government approach that is based across four essential pillars – capability, credibility, communication, and competition – on a foundation of comprehension (Ref. [7], p. 3). These pillars must all combine to create a deterrent effect on an adversary and if any one fails, so too does the deterrent effect. The Integrated Operating Concept 2025 recognises the vital role Defence plays in protecting the homeland and the importance of enhancing domestic resilience in the contemporary security environment. The ability to suffer a set-back, continue to operate and recover back is essential and through enhancing resilience, by making it more difficult to cause damage and disruption, deterrence through denial is achieved. Developing effective resilience however requires a multifaceted approach and must be applied to the full breadth of Defence, from training and education through to logistics, infrastructure, and communication systems. The current UK approach does not disregard the importance of resilience and deliberate measures are taken to reinforce it but successive cuts to the Defence budget and size of the Armed Services since the end of the Cold War have left very little 'fat' in the system.

The issue of decreasing redundancy as tighter budgets force a greater focus on developing efficiencies poses a serious challenge. Efficient does not mean effective and the shifts in the threat landscape in an era of persistent competition within the international system with varied and intensifying threats represent a challenge to established responses. The UK, along with its allies and partners must remain adaptable to meet new challenges and be open to incorporating new methods and ways of doing things. On matters of resilience, a point that was brought out earlier in the chapter is the need for better public engagement in defence. Mass participation helps create resilience and the most effective way of delivering this in the UK is through mass communication (Ref. [5], p. 24). Debate about strategy should not be confined to elites and allowing the public to develop a proper understanding of the issues that govern the utility of military force will be important in being able to identify new ways to meet the identified new challenges.

The role of the Reserves represents one area where new threats to national security may force a change in responsibilities. COVID-19 has been illuminating in the demand for more complex and skilled homeland defence tasks from logistics to medical support and the ability of the military to provide them. The Reserves may be central to a bolstered Homeland Resilience contribution, dropping their expeditionary role to be ready to deploy at home. It is too early to tell whether there will be significant policy changes to the Reserve model in the UK but the demand signal and appreciation that homeland tasks are likely to increase in importance and frequency is growing. The incorporation of Reservists in security support at the local and regional level certainly deserves more consideration than it is used to receive (Ref. [5], p. 25).

On a more general note, better integration of the Armed Forces within the community will contribute to enhanced resilience. Large swathes of the UK have very little military representation due to efficiencies of concentrating forces in certain parts of the country, but such a situation need not be the case. Forces employed on MACA tasks offer a valuable opportunity to familiarise the public with the military who may otherwise seem remote and contribute to an enhanced awareness of resilience and its role in domestic security (Ref. [5], p. 25).

8.3.3 Part 2 Summary

The UK's almost exclusive focus on MACA is an important aspect of how resilience is understood within Defence and wider society. The relatively narrow focus has its roots in events from the early 2000s but there is a strong argument to suggest the world has changed and resilience tasks have grown in complexity and scale in line with new and emerging threats. Successive Defence cuts raise important questions about whether adequate resources can be allocated to resilience tasks as part of a Comprehensive National Defence System, especially if other outputs tied to NSOs and 'Global Britain' are sustained. New and emerging challenges cannot be ignored and as a result it is clear different ways and new approaches must be identified.

8.4 PART 3: MAKING THE CHANGE

Bold statements about how change needs to be applied are fraught with risk and caution needs to be exercised, especially in a deliberately brief case study. Nevertheless, this chapter has outlined in big handfuls the UK's approach to how it is organised for domestic security tasks and where the Defence contribution to resilience lies. The challenges of implementing a Comprehensive National Defence System are significant but a good starting point will be to create and sustain public dialogue.

8.4.1 Challenges of Implementation

Societal perception is perhaps the greatest challenge of implementation. This chapter has already referenced the traditional caution the British state has shown towards a standing army and its use domestically. Although, there is increasing evidence to suggest the perception of the people towards the military in recent years is largely positive and their employment in domestic tasks is generally widely supported, a consistent theme emerges that emphasises the following conditions: any deployment must be proportionate to the threat; must remain subordinate to the Civil Power; should be used as a last resort; and to a lesser extent is short term in nature (Ref. [1], p.7). Public buy-in and trust are essential components of creating a Comprehensive National Defence System and need to be treated delicately. Change cannot happen overnight and can be extremely slow to embrace change. The most effective way for the UK model to adapt its current approach to domestic security and resilience is to widen the debate and seek greater public input rather than leaving matters of defence and security almost exclusively in the hands of political elites.

A related challenge to that of societal perception is one of resource and will. Like many of its NATO allies and partners, the UK has steadily reduced the size of its Armed Services since the end of the Cold War. The army today is the smallest it has been since Napoleonic times and yet it has to operate in a world that has never been more interconnected and volatile. Institutions like Defence have traditionally been resistant to change at the best of times but under current circumstances when resources are scarce and likely to be made more so following COVID-19, it is difficult to imagine a revised posture that could threaten more established military capabilities or formations. Added to this is the importance of will. If the hierarchy and decision-makers do not recognise vulnerabilities the new security context presents, there is little incentive to drive through change.

Before concluding the final point concerns the aftermath of COVID-19. The pandemic has been a massive global shock that is still ongoing and the world after it is likely to be very different. It is too early to establish with any certainty what that world will look like and where real change will have taken place. Civil-military cooperation is likely to be closer than before and COVID-19 may be the event that encourages change in the UK with a renewed focus on resilience and what this means.

8.5 CONCLUSION

This chapter has outlined the dominant security challenges the UK is likely to face over the next decade and how they relate to the NSOs as presented in the NSCR. The NSOs present a clear ambition and tied to aspirations of 'Global Britain' offer a coherent and realistic perspective of the UKs place in the world. However, the notion of a Comprehensive National Defence System is an unfamiliar construct to the British state who have traditionally opted to 'defend away' and tackle threats to national interest at their source. Fusion Doctrine is the latest framework to cohere a cross-government response to securing national interests but remains an evolving model through which Defence must play an active part. The conceptual underpinning is moving in the right direction, but it is unclear whether there is an appetite for a truly Comprehensive National Defence System. JDP 02 almost exclusively deals with MACA and how Defence is used in response to requests from the Civil Power and even with JDP 0-01 in support, fails to consider the myriad of threats across multiple domains that the Integrated Operating Concept 2025 give emphasis to. Resilience and redundancy are key challenges for domestic security and to resource this is an imaginative and innovative way, a positive societal perception of the military must be a priority to move closer to a Comprehensive National Defence System.

8.6 REFERENCES

[1] Harding, J. 2020, "Continuity or change? Managing cultural preferences for the use of the Armed Forces for domestic security in the UK", Internal DCDC Report. https://www.gov.uk/government/groups/development-concepts-and-doctrine-centre. Accessed 5 Apr 2020.

[2] HM Government (2018), "National security capability review, (Crown Copyright)". https://www.gov.uk/government/publications/national-security-capability-review-nscr, Accessed 16 April 2020.

[3] Jeffrey, K. (1985), "Military intervention in democratic societies", Chapter 2 in P.J. Rowe, and C.J. Whelan (Eds.), Military Aid to the Civil Power in the United Kingdom – An Historical Perspective, Croon Helm: Kent.

[4] Lawson, E. (2018), "RUSI, The UK national security capability review and the fusion doctrine", https://rusi.org/commentary/uk-national-security-capability-review-and-fusion-doctrine, Accessed 17 May 2020.

[5] Strachan, H. (2020), "The utility of military force and public understanding in today's Britain", RAND Europe. https://www.rand.org/pubs/research_reports/RRA213-1.html, Accessed 30 May 2020.

[6] UK Ministry of Defence, Development Concepts and Doctrine Centre (DCDC), "2017, Joint Doctrine Publication 02 (JDP 02), UK Operations: The Defence Contribution to Resilience and Security", 3rd Ed., (Crown Copyright). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/591639/20170207_JDP02_Resilience_web.pdf, Accessed 2 Apr 2020.

[7] UK Ministry of Defence, Development Concepts and Doctrine Centre (DCDC), "2020, Integrated operating concept 2025, (Crown Copyright)". https://www.gov.uk/government/publications/the-integrated-operating-concept-2025/the-integrated-operating-concept-2025-accessible-version, Accessed 8 Apr 2020.[2]

[8] UK Ministry of Defence, Development Concepts and Doctrine Centre (DCDC), "2018, Global strategic trends 6". (Crown Copyright). https://www.gov.uk/government/publications/global-strategic-trends, Accessed 10 Apr 2020.

[9] UK Ministry of Defence, Development Concepts and Doctrine Centre (DCDC) (2020), "2020, A post vaccine COVID 19 Paper", (Crown Copyright). Internal DCDC Report. https://www.gov.uk/government/groups/development-concepts-and-doctrine-centre. Accessed 15 Apr 2020.

[10] UK Ministry of Defence, Development Concepts and Doctrine Centre (DCDC) (2014), "Joint Doctrine Publication 0-01 (JDP 0-01) UK Defence Doctrine", 5th Ed., (Crown Copyright). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/389755/20141208-JDP_0_01_Ed_5_UK_Defence_Doctrine.pdf Accessed 6 May 2020.

[11] Wendling, C. (2010), "The comprehensive approach to civil-military crisis management: A critical analysis and perspective", IRSEM, p.72. https://gisf.ngo/wp-content/uploads/2014/09/0155-Wendling-2010-Comprehensive-approach.pdf, Accessed 28 May 2020.

[2] The IOpC25 was originally published in May 2020 and the current draft has been retracted with minor amendments due to be released in conjunction with the Integrated Review (date TBC). The ideas taken from the IOpC25 in this paper remain valid.

Chapter 9 – COMPREHENSIVE NATIONAL DEFENCE: COVID-19

Erdal ARSLAN
Selcuk University
TURKEY

9.1 INTRODUCTION

As it is known, the COVID-19 epidemic, caused by the corona virus, which emerged in China and spread to many countries, was declared a pandemic by the World Health Organization (WHO) on 11th March 2020. In this context, the process outlined in the following sections was performed within the framework of Comprehensive National Defence for COVID-19 epidemic in Turkey.

9.2 STUDIES IN THE FIELD OF HEALTH

To battle the COVID-19 epidemic; Hadımköy Dr. İsmail Niyazi Kurtulmuş Hospital, Prof. Dr. Murat Dilmener Emergency Hospital and Prof. Dr. Feriha Öz Emergency Hospital were put into operation. Başakşehir Çam and Sakura City Hospital was opened.

For the follow-up of the disease, radiation teams with a total number of 6239 people working 24 hours a day, 7 days a week, were established. Health workers travelled door-to-door throughout the country, following the new type of coronavirus. The aim was to identify and quarantine COVID-19 patients and those contacting them, thereby preventing the spread of the virus. In Turkey, one of the strategies implemented against the coronavirus epidemic, was determining virus exit points with an affiliation method instead of making the general public test for COVID-19. Thus, attempts were made to prevent the epidemic from spreading in a city, neighbourhood, or street. As soon as the case occurred, teams of two or three people scanned for 48 hours. Teams that reached the address directly established a new network against the disease in each new case.

In Turkey, the first case was seen in the 11 March 2020. As of 19 March, the number of tests started to be announced. In this context, it was announced that 1981 tests were carried out on March 19, 2020. On 31 May 2020, the number of tests was 2,039,194.

Based on the 356th and 508th articles of Presidential Decree No. 1 published on 10 July 2018 by the Ministry of Health on March 18, 2020, the Hospital Disaster and Emergency Plans Implementing Regulation was issued.

With the Regulation published on 22 April 2020, COVID-19 (new coronavirus disease) was added to the Notification List of Infectious Diseases.

9.3 PRESIDENTIAL CIRCULAR AND PRESIDENT'S DECISION

Under the Presidential Circular dated 13 March 2020, all public officials were stopped from going abroad in order not to cause any problems in the execution of public services.

Under the Presidential Circular of 20 March 2020, all kinds of scientific, cultural, artistic, and similar meetings or activities to be held in open and closed areas at national and international level were postponed until the end of April.

Under the Presidential Circular dated 22 March 2020, flexible working methods such as working remotely, alternating work were introduced to those working in public institutions and organisations.

With the President's Decision dated 13 April 2020, it was decided that personal protective equipment provided by the Ministry of Health for virus protection, tests used in the diagnosis of the disease, as well as kits and medicines used in the treatment of the disease would be free for all people affected by coronavirus.

With the President's Decision published on 17 April 2020, the military service period of soldiers and soldiers who were armed between 1 November 2019, and 1 December 2019, was extended by one month.

Under the Presidential Circular of 29 May 2020 and the Circular on Permission to Go Abroad of Public Officials of 13 March 2020 and the Additional Measures for Public Employees within the Scope of COVID-19 of 22 March 2020 were repealed.

9.4 DECISIONS TAKEN BY THE RELATED MINISTRIES

The measures taken by the relevant Ministries in the struggle against COVID-19 follow.

9.4.1 Precautions at Border Gates

In the circular published by the Ministry of Internal Affairs dated 13 March 2020; Within the scope of the recommendations of the Ministry of Health and the Scientific Committee, it was stated that various precautions have become mandatory for Austria, Belgium, Denmark, France, Germany, the Netherlands, Norway, Spain, and Sweden, where the epidemic has spread rapidly. In the circular sent by the Ministry of Interior to 81 provinces, the following measures were taken at the border gates:

- Passenger entries from these countries to our country were stopped at all border gates.
- The citizens of the mentioned country and the citizens of the third countries in these countries in the last 14 days will not be admitted to our country from 08:00 on 14 March 2020.
- Citizens of those countries will not be any restrictions on exit from Turkey.
- Travels to these countries, citizens of the Republic of Turkey temporarily stopped.
- Regarding the mentioned countries, as in China, Iran, Iraq, Italy, and South Korea, according to the procedures and principles set by the Ministry of Health; 14-day surveillance and quarantine operations will be made if necessary.
- On 14 March 2020, it was decided to close the Sarp border gate to passenger traffic.

In the circular published by the Ministry of Interior on 15 March 2020; it was stated that the pavilions, discotheques, bars, and night clubs would be temporarily shut down as of 16 March, 10:00.

9.4.2 Limitations to Public Institutions

Those pregnant women working in public institutions and organisations, those who use the legal milk permit, disabled people, those who are 60 years of age except those in executive positions and over were considered as taking 12 days administrative leave from 16 March. Female officers with children in preschool and primary education were granted annual leave. In addition, the departure of public officials abroad was made subject to special permission [1].

9.4.3 Education and Training

As of 16 March 2020, primary, secondary, and high school schools were vacationing for 1 week and universities for 3 weeks. In this context, as of 23 March 2020, necessary infrastructure preparations had been completed in order to continue education on internet and television channels via distance education method.

In addition, the dates of the academic exams such as Academic Graduate Education Exam and Foreign Language Exam were postponed to a later date by updating the exam schedule by the Student Selection and Placement Centre. In later statements, it was reported that the period would be completed with distance education in primary, secondary, and high school and universities [1].

9.4.4 Restriction to Social Activities

As of 17 March 2020, 00:00, theatres, cinemas, show centres, concert halls, engagement/wedding halls, restaurant / café with music, music, casinos, pub, tavern, coffeehouse, café, cafeteria, country garden, hookah lounges, hookah cafés, internet lounges, internet cafés, all kinds of game rooms, all kinds of indoor playgrounds (including shopping malls and restaurants), tea gardens, clubhouses, amusement parks, swimming pools, Turkish baths, saunas, spas, massage parlours, SPA and sports activity centres were temporarily suspended [1].

The letter sent to the Governorships by the Ministry of the Interior on 21 March 2020 stated that the soldier farewell ceremonies in which the citizens participate collectively would increase the risk of coronavirus epidemics. In addition, in the letter sent to the Governorships; many different measures were taken, such as stopping activities in some public places where citizens were present, delaying gatherings such as weddings, conferences, seminars, etc. temporarily [1].

9.4.5 Restriction to Restaurants

Under the circular issued by the Ministry of Internal Affairs on 21 March 2020, all restaurants with drinks and/or non-alcoholic drinks, patisseries and similar establishments will serve only takeaway, take-out, without allowing customers to sit down. For this reason, restaurants, patisseries, and similar workplaces will be required to remove seating areas, and necessary actions will be taken to prevent them from accepting customers [1].

9.4.6 Restriction of Activities of Barber, Hairdresser, Beauty Centres

Under the circular issued by the Ministry of Interior, it was decided to temporarily cease the activities of barbers, hairdressers, and beauty centres as of 21 March 2020, 18:00 [1].

9.4.7 Curfew Restriction for Citizens over 65 and Chronic Disease

Under the circular issued by the Ministry of Internal Affairs on 21 March 2020, should people aged 65 and over and those with low immune system, chronic lung disease, asthma, COPD, cardiovascular disease, kidney, hypertension, and liver disease and those using drugs that disrupt the immune system wish to leave their residence they were restricted from travelling in open areas, parks and travelling by public transportation, and were prohibited from going out on the streets. In particular, to meet the basic needs of citizens aged 65 and over and those with chronic illness living alone and without relatives to meet their needs, it was decided to establish the Vefa Social Support Group over 65 years under the chairmanship of governors/district governors. (With the additional circular sent to the Governorships by the Ministry of Interior, exceptions to be introduced within the scope of the curfew imposed on people aged 65 and over and those with chronic illnesses were specified. In this context, exemptions have been brought to healthcare professionals, especially doctors, mayors, provincial directors, officers of social service organisations, public service providers and pharmacists) [1].

9.4.8 Flight Prohibitions

With the announcement made by the Ministry of Transport and Infrastructure on 21 March 2020, it was stated that flights to 46 countries will be stopped in addition to 22 countries where the flights were previously stopped. In Turkey, 68 countries had closed its air traffic: Algeria, Angola, Austria, Azerbaijan, Bangladesh, Belgium, Cameroon, Canada, Chad, China, Colombia, Czech Republic, Denmark, Djibouti, Dominica, Ecuador, Egypt, Equatorial Guinea, Finland, France, Georgia, Germany, Guatemala, Hungary, India, Iran Ireland, Iraq, Italy, Ivory Coast, Kazakhstan, Kenya, Kosovo, Kuwait, Latvia, Lebanon, Mauritania, Moldova, Mongolia, Montenegro, Morocco , Nepal, Netherlands, Niger, North Macedonia, Norway, Oman and Jordan. , Panama, Peru, Philippines, Poland, Portugal, Saudi Arabia, Slovenia, South Korea, Spain, Sri Lanka, Sudan, Sweden, Switzerland, Taiwan, TRNC, Tunisia, Ukraine, United Arab Emirates, United Kingdom, and Uzbekistan. Libya, Qatar, and Russia took a unilateral decision to discontinue flights to Turkey. Thus, the total number of countries whose air traffic was cut reached 71 in total. In addition, in the statement made by Turkish Airlines on 22 March 2020; it was stated that all international flights except those to Addis Ababa, Hong Kong, Moscow, New York and Washington were terminated from 27 March 2020 until 17 April 2020 [1].

9.4.9 Bank Working Hours

The Banks Association of Turkey decided to make a recommendation for the working hours of all banks, which was taken by the Union on 22 March 2020. Upon the recommendation of the Banks Association of Turkey, the working hours of branches and customer service units providing direct services to clients of banks were determined to be 12:00 – 17:00. Apart from this, it was decided that banks could determine flexible working and customer acceptance hours and that the banks would inform the customers about the working and customer acceptance hours. In addition, decisions were made to ensure that branches in high-risk and crowded areas could be kept out of service, and that banking services were available through digital media [1].

9.4.10 City Entry/Exit and Age Restrictions

On April 3, 2020, city entry/exit measures and age restrictions were introduced. Accordingly:

- All entrances/exits from 30 provinces with metropolitan status and Zonguldak provincial borders by land, air, and sea (public transport, private vehicle, and pedestrian, etc.) were stopped for a period of 15 days starting from 24:00 on 03 April 2020.
- It was essential for all citizens living/staying in these provinces to stay in their provinces for the specified period.

In addition, to cover 81 provinces:

- In all of our provinces and districts, those who were born after 01 January 2000 were temporarily banned from going out onto the streets from 03:00 on 20 April 2020.
- Additional measures to be taken to minimise urban mobility in all provinces from 24:00 on Friday, April 03, 2020, to be discussed at the Provincial Pandemic Board. The issues recommended by the Provincial Pandemic Board to be decided by the Provincial/District Public Hygiene Boards and to be implemented.
- In our provinces and districts, our citizens and employees to wear masks to enter the market place, market, and collective workplaces.
- In the squares and streets in our provinces and districts; citizens would not be allowed to walk or meet together, regardless of social distance. Attention to be drawn to our citizens walking side by side considering the social distance.

9.4.11 Keeping Foreigners in Quarantine

77441 citizens from 97 countries were quarantined in dormitories affiliated with the Credit and Hostels Institution and this process was completed as of 3 June 2020.

9.4.12 Helping Countries

Turkey's assistance began with receiving calls for aid from 116 countries. Aid was delivered to 44 countries. Aid sent to Iran on 17 March included 1,000 diagnostic kits, 4,715 overalls, 20,000 gowns, 2,004 glasses, 4,095 masks and 78,000 trifold masks. In addition to 20,000 masks delivered to Erbil on the day of the outbreak, 30,000 masks and 475 parcels of food were provided to Iraq. On 1 April 2020, an aircraft belonging to the Turkish Armed Forces delivered health supplies consisting of mask overalls and anti-bacterial fluid to Italy and Spain, which were among the countries most affected by the coronavirus and who could not receive assistance from EU countries. In the statement made by NATO, it was stated that among the materials sent were 450,000 masks in total for the two countries. Aid materials were also sent to many Balkan countries. Medical aid supplies were sent by military cargo plane to Serbia, Kosovo, Bosnia and Herzegovina, Montenegro, and North Macedonia on 8 March. The Kosovo Red Cross shared the Red Crescent's aid report and announced that 63,000 medical supplies worth TL 160,000 were sent. Among those countries receiving donations were developed states like the UK. Medical aid support was provided to some of the richest countries in the world, starting on 10 April 2020. In addition, the USA, which had become the centre of the epidemic, with increasing number of cases and mortality rates, was also included in the scope of aid. The first package of aid, containing masks, overalls, and protective materials, was delivered to the USA on 28 April and the second on 30 April. British officials stated that the aid delivered through NATO included 250,000 sets of personal protective equipment on one of the two military cargo aircraft. US authorities in various countries receiving assistance from Turkey in Ankara sent thank you messages and expressions of gratitude. Overall, 44 countries, including Georgia, Azerbaijan, Colombia, and Pakistan, benefited from the aid. In the aid sent, it was stated that the most supplies were distributed. The packs were announced to include masks, overalls, preservatives, glasses, gloves, and the COVID-19 test kit. Medical aid materials were sent to Colombia, including 26,250 test kits. Aid provided included Mosque cleaning and disinfection in Indonesia, hospital grants in Gaza, renovation of the health centre in Romania, donation of a 3D printer in Sudan, and training of healthcare workers in Yemen [2].

9.4.13 Establishment of the Scientific Committee

The Ministry of Health Coronavirus Scientific Board was established as an advisory board on 10 January 2020 to battle the COVID-19 epidemic. The Assembly of 31 people included university academics working as medical scientists in the fields of infections, microbiology, virology, internal medicine, intensive care, and respiratory diseases. Turkey's Health Minister served as chairman of the board. After the first death on 9 January 2020, in Wuhan, the "2019-nCoV Disease Guide" prepared by the Scientific Board was published by the Ministry of Health on 14 January. The guide includes general information about the care and isolation of patients, the conditions required to identify the case, and procedures to be followed after identification of the virus. Following new information and developments, this guide was updated after the Science Board meeting, on 28 January. On 2 February, the guide was published on the website as a result of the decision taken after a meeting [3].

Turkey passed the Emergency Management on 6 April 2020. In this framework, intercity traffic restrictions were introduced, and urban traffic was reduced. Within the framework of emergency management, interventions were made when groups of people gathered in crowded centres such as squares and main streets in big cities. In certain cities, main streets were closed to pedestrian traffic, and quarantines were implemented in some districts, cities, villages, and hamlets, including city centres [4].

9.5 DECISIONS TAKEN IN THE FIELD OF ECONOMICS

9.5.1 Economic Decisions for Companies

- April, May and June payments of the concise and VAT withholding, and SSI premiums postponed for 6 months for the Retail, Shopping Mall, Iron-Steel, Automotive, Logistics-Transport, Cinema-Theatre, Accommodation, Food-Beverage, Textile-Garment and Event-Organisation sectors.
- The easement rights and revenue share payments related to hotel rentals were postponed for 6 months for April, May, and June. The accommodation tax not to be applied until November.
- In domestic air transport, the VAT rate reduced from 18 percent to 1 percent for 3 months.
- Credit capital payments and interest payments to the banks of the companies whose cash flow is impaired due to COVID-19 epidemic precautions to be delayed for a minimum of 3 months and additional financial support to be provided if necessary.
- In order to maintain capacity utilisation rates during the temporary slowdown in exports, exporters to be provided with stock financing support.
- In this period, the credit debts of the tradesmen and artisans who demanded by declaring that their works were adversely affected, Halkbank's April, May and June principal and interest payments to be postponed for 3 months and without interest.
- Credit Guarantee Fund limit to be increased from 25 billion liras to 50 billion liras. In the loans to be given, priority to be given to companies with liquidity needs and collateral deficits and to SMEs.
- With the effect of virus precautions, firms that default in April, May, and June to have a "force majeure" grade in their credit registry.
- Tax declarations, including payments of deductions made at the source such as withholding, to be delayed for 3 months.
- Minimum wage support to continue.
- Flexible and remote working models in the legislation to be made more effective.
- Short Work Allowance to be put in place, the processes required to benefit from this to be facilitated and accelerated. Thus, while temporary income support is given to workers at workplaces that interrupt their activities, the cost of employers will be reduced.
- Alternative channels to be developed according to the priorities determined in both production and retail in case of a failure in global supply chains.
- Necessary support to be given to Turkish Airlines.

9.5.2 Economic Decisions Made for Citizens

- The introduction of social credit packages to be encouraged under appropriate and advantageous conditions for citizens.
- In houses under 500,000 lira, the credible amount to be increased from 80% to 90%, the minimum down payment to be reduced to 10%.
- The lowest pension to be increased to 1,500 pounds.

- The holiday bonus of retirees to be paid at the beginning of April. Again, pensioners' salary promotion payments to be provided directly to their accounts, without the need to go to branches. Public Banks to pay the salaries of people over the age of 76 to their homes if they wish.
- According to the criteria set by the Ministry of Family, Labour and Social Policies, an additional 2 billion lira resource to be allocated for financial aid to families in need.
- In order to ensure continuity in employment, the 2-month compensatory working period to be increased to 4 months.
- Periodic follow-up program consisting of social and home health services to be launched for the elderly people over 80 years old living alone.
- The number of doctors in nursing homes will be increased, and the health of the elderly to be closely monitored.
- With the work to be started in Istanbul and Ankara, protective masks, and cologne to be distributed to all elderly people over 65 years old.

9.6 REFERENCES

[1] Campaign Türkiye (11 March 2020), "COVID-19 salgınına karşı alınan tedbir ve önlemler", https://www.campaigntr.com/covid-19-salginina-karsi-alinan-tedbir-ve-onlemler/

[2] Politikaakademisi.org (18 May 2020), "Pandemi sürecinde türkiye'nin diş yardimlari", http://politikaakademisi.org/2020/05/18/pandemi-surecinde-turkiyenin-dis-yardimlari/ (accessed 3 June 2020).

[3] Milliyet.com (06 April 2020), "Bilim Kurulu üyeleri kimlerdir, isimleri nedir? 2020 Koronavirüs Bilim Kurulu üyeleri kimlerden oluşmaktadır?", https://www.milliyet.com.tr/gundem/bilim-kurulu-uyeleri-kimlerdir-isimleri-ne-2020-bilim-kurulu-uyeleri-kimlerden-olusuyor-6180779 (accessed 6 April 2020).

[4] Yetkin, M. (06 April 2020), İçişleri Bakanı Soylu: "Acil Durum" yönetimine geçtik [Yetkin Report]. https://yetkinreport.com/2020/04/06/icisleri-bakani-soylu-acil-durum-yonetimine-gectik-2/

Chapter 10 – COLLABORATIVE DEFENCE: EXPLORING RELATIONS AND EXPECTATIONS BETWEEN SOCIETY AND DEFENCE

Joaquim Soares
Belgian Defence Strategy Department
BELGIUM

Geert Letens
Royal Military Academy
BELGIUM

William Demeyere
Control and Reporting Centre
BELGIUM

DISCLAIMER

The views expressed in this document are the sole responsibility of the authors and do not necessarily reflect the official positions of the Royal Military Academy, the Belgian Defence Strategy Department, the Belgian Ministry of Defence, or the Belgian Government.

10.1 INTRODUCTION

NATO countries are facing an important strategic security challenge: how to steer defence and security policy in light of the challenge posed by the VUCA environment [5], [59]? As current security policies often fall short because they fail to adequately cope with this environmental complexity and uncertainty [16], [19], there is a need to develop new approaches to better steer this field of public policy.

Some of the reasons and challenges underlying the need for new approaches have previously been identified in this report. First, modern threats far exceed the traditional boundaries of military defence as non-military means are increasingly used to achieve political and military goals [8]. For example, our complex, integrated, and interdependent societies are vulnerable to disruption by terrorist, cyber, or hybrid attacks across a broad range of critical sectors and services. Services, which may be impacted independently or concurrently, include energy, health, transportation, finance, IT, water, food, the chemical industry, the nuclear industry, public and legal order, and aerospace amongst others. There is therefore a need to reduce the total number of vulnerabilities an enemy can leverage across a wide set of critical domains. In turn, this implies a crisis management system built on common situational awareness and close cooperation between different stakeholders [39]. At the same time, when exploring the means available, it appears that single-agency outputs are limited, meaning that a cross-domain utilisation of resources is indispensable to achieve significant effects as may be desired when navigating a major or complex crisis [39], [51]. Joint or coordinated use of resources, in turn, requires such tools and processes as joint C2, joint financing mechanisms, joint plans and joint strategies which also render a certain degree of collaboration between stakeholders indispensable.

Overall, the existing threats and the limited means imply a whole-of-society approach to national defence where different governments, ministries and organs of society cooperate in a coordinated manner across multiple aspects of social life to reduce vulnerabilities, increase resilience, resist foreign intervention and defeat aggression [5], [8]. As part of this effort, and within Government itself, horizontal coordination between public authorities and institutions is primordial and is sometimes referred to as the Whole-of-Government approach. Whether on a Governmental or Societal level however, successful cooperation and coordinated effects implies the development of good insight on defence stakeholders and their actions [59].

Various frameworks have therefore emerged over the years in different countries all aiming to improve the amount and intensity of societal and horizontal government cooperation. However, it appears from practice that cooperation could still be improved. For example, Peets [45] draws attention to shortcomings in planning, situational awareness, and cross-sector exchange of information. According to Berzina [8], not only is this capability to cooperate amongst stakeholders important as such but, the overall architecture of the societal network may be crucial in determining the overall level of assistance to Government and force structures in overcoming any crisis, including military conflicts. Within the military itself, and according to Boylan [9], the ability to share information and successfully influence various stakeholders is insufficient at this time. This implies that more attention needs to be placed to better understand the different defence stakeholders and the overall defence stakeholder network which is the focus of this study.

Our study is unique due to the fact that it is based on a selection of 199 high quality empirical studies which were previously dispersed in the literature. After proposing a classification of the most important stakeholders into larger stakeholder groups, we examine the contexts and frameworks wherein the different stakes materialise. In doing so, we identified Total Defence as the most studied framework that also exhibits the highest number of linkages with the different stakeholder groups, which testifies to its holistic nature and possible emergence as a baseline for future comprehensive national defence initiatives. We further explored the implications for defence organisations wanting to leverage the stakeholder network across several factors such as the country, the armed force type (or the ambition level) and the performance measurement maturity level of the organisation. In identifying countries that are likely more advanced in the field, we proposed that more ambitious armed forces make greater use of performance measurement and management techniques and may be better placed to leverage their stakeholder network. At the same time, we proposed that defence organisations wanting to expand their stakeholder network had to synchronise this ambition with their own internal stakeholder engagement capability. Ultimately, harnessing empirical knowledge on the politico-strategic stakeholders and stakeholder network should help nations address the gap between stakeholder contributions and stakeholder satisfaction as highlighted in existing NATO research [22].

Following this introduction, we propose a background and theory section to lay the foundation for the remainder of the chapter. The research objectives are then summarized leading to an explanation of the systematic literature review methodology used and the analysis of A1 papers pursued. The main findings are then followed by a discussion and managerial implications section. Finally, we conclude with the conclusions section and some avenues for future research.

10.2 BACKGROUND AND THEORY

As comprehensive national defence requires an orchestrated effort of different stakeholders to achieve desired results in solving complex problems in an uncertain and volatile environment, the first question that cropped up is: what is meant by the concept of stakeholder? For the purpose of this study, we used the most commonly used definition of a stakeholder as originating from Freeman [21]: “any group or individual who can affect or is affected by the achievement of the organisation’s objectives”.

As is pointed out by the Murumets and Ermus [39], based on such a broad definition, it is easier to list those who are not stakeholders of defence than describe the variety of groups, organisations, and persons, who are affected by the comprehensive national defence concept. As the study of an exhaustive list of stakeholders is out of the scope of this study, we appeal to the concept of stakeholder groups as an attempt to regroup and simplify some of the ecological complexity in this field. This concept, which has been used in other studies [19], [39], consists of grouping the most important stakeholders together according to similar characteristics such as common intent. In doing so, we developed the following list of stakeholder groups depicted in Table 10-1 which was also presented to academicians at the Institute of Industrial and Systems Engineers Annual Conference 2020 held in New Orleans, U.S.A.

When comparing our table to other studies that have made a similar attempt to categorise stakeholders, we see that the classification is similar even if national specificities can influence the list. For example, in the case of Estonia [39], the Home Guard is mentioned as a separate stakeholder and the population includes foundations, charities and civic groups explicitly. In the case of Norway [19], the defence establishment is broken down into different sub-entities (Home Guard, Norwegian Defence Research Establishment, etc.), hospitals are made part of private companies (whereas we consider it part of first responders) and the population mentions faith groups and clubs explicitly. As all these actors differ from each other based on such parameters as objectives, working culture, organisational design, and responsibilities, they all deserve their own detailed study on their relationship and expectations with respect to the defence organisation. Some references from their body of literature are provided in Table 10-1 none the less.

Table 10-1: Stakeholder Groups.

Stakeholder Group	Examples	References
Internal stakeholders	Categories of military personnel (women, minorities,, etc.), civilian personnel, deployed personnel, etc.	[43], [15], [1], [53]
Government including federal departments and ministries	Head of Government, Head of State, National Government/Council of Ministers, Ministry of Interior, Ministry of External Affairs, Ministry of Justice, International Development, Intelligence Agency, National Space Agency, Environment Ministry, Ministers, National Security Council, Cabinet-level staff, etc.	[46], [31], [4], [41]
First responders	Police, Fire Brigade, Civil Protection, Ambulance Service, hospitals, Local Authorities, etc.	[58], [25], [39]
Coordinating bodies	Cyber, intelligence, crisis management, Prime Minister's Office, National Security Council, etc.	[18], [3], [32], [30]
Political stakeholders	Regional entities, Party leaders, Members of Parliament, Parliamentary Commissions, local politicians, institutions in deployed areas, etc.	[17], [18], [30], [56]
Population	Reservists, veterans, local population in deployed areas, home-based population, etc.	[50], [57], [35]
Partner countries	Alliance members, bi-lateral cooperation, multi-lateral cooperation, regional bodies (NORDEFCO, BENELUX, VISEGRAD, etc.), Security Force Assistance (SFA) programs, etc.	[13], [53], [54], [36]
International organisations	NATO, EU, UNO, OSCE, etc.	[47], [42], [48], [54]
Private companies	Industry, Private Military and Security Companies (PMSC), outsourcing partners, etc.	[7], [52], [5], [19], [59]
Humanitarian organisations	Home-based (National Red cross), Foreign-based (MSF, ICRC, WHO, etc.)	[28], [34], [2]
Competition and threat	Competing country, terrorist organisation, insurgents, etc.	[11], [37], [6]
Media	Home-based media (social and traditional), media in deployed areas (social and traditional)	[27], [20], [40], [8]

We further attempted to conceptualise the fit between these stakeholder groups and the different comprehensive national defence frameworks more or less loosely mentioned in the literature. In doing so, we were able to identify several different types of frameworks as depicted in Figure 10-1.

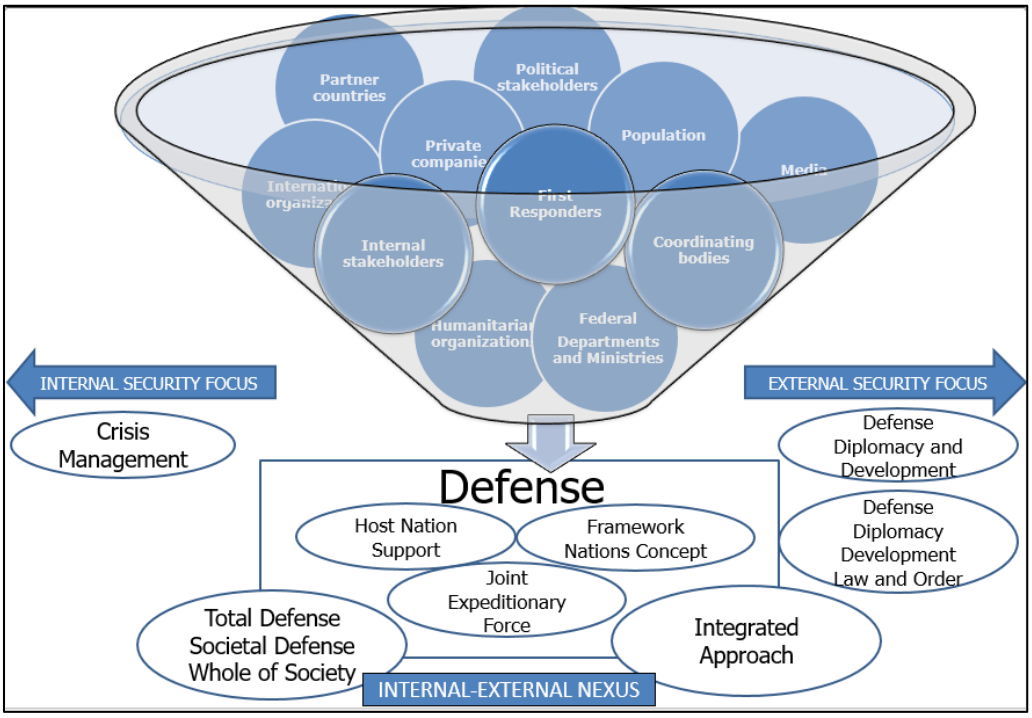

Figure 10-1: Stakeholder Frameworks.

First, we identified frameworks that tend to focus on stakeholder groups more involved in internal security (such as first responders in the case of crisis management and disaster response). Second, we identified frameworks that tend to focus more on stakeholders active in the field of external security (mainly Foreign Affairs and International Aid and Development as in the case of the 3D approach and its derivatives). Third, we identified frameworks that seemed to be more linked to stakeholder groups such as partner countries and international organisations (such as NATO with its Host Nations Support and Framework Nations Concepts). Last and importantly, there seemed to be a set of frameworks, such as Total defence, where the aforementioned cleavages seemed to disappear and where all our stakeholder groups could potentially fit.

10.3 RESEARCH OBJECTIVE AND QUESTIONS

Given the previously described trends and challenges, our main research objective is to better understand and identify the different stakeholder groups and frameworks mentioned in the literature and explore what the implications may be for the demonstration of military performance towards these stakeholders from a defence organisations' perspective. This research objective can, in turn, be broken down into the three following research questions:

- What are the main strategic-level societal stakeholder groups mentioned in the literature?
- In which frameworks and contexts do they have expectations and relationships with defence?
- What are the factors that influence the stakeholders' network?

10.4 RESEARCH METHODOLOGY

10.4.1 Data Collection

For the purpose of this study, we exploited the results of an available systematic literature review conducted in cooperation with the University of Central Florida along a process shown in Figure 10-2 [29]. While the process was similar to the one followed in the 1st chapter of the phase one report, the main difference lies in the fact that a new platform was selected for this study being Web of Science. This is also reflected in the Figure 10-3. The platform-specific exclusion criteria used included the exclusion of certain terms such as gender and virus, the exclusion of particular domains such as agriculture and physics, the restriction to languages understood by the researchers being English, French and Dutch and the restriction to journal articles and readily available book chapters. This yielded a total number of 10251 search results out of which a total of 1411 papers were retained based on title and abstract vetting for general relevancy. Out of these 1411 papers, 1303 were retrieved in pdf format following several attempts across multiple platforms including Web of Science, Google Scholar and Research Gate.

We then applied stricter exclusion criteria thereby only retaining A1 empirical documents with a focus on:

1) NATO, the EU, or a Member State of one of these two institutions;
2) Defence or military matters;
3) The strategic-level of the organisation; and
4) At least one stakeholder.

We scanned the full paper for this purpose which yielded a total of 199 papers. We also added 7 documents previously obtained from experts in the field bringing our final paper set to a total of 206 papers.

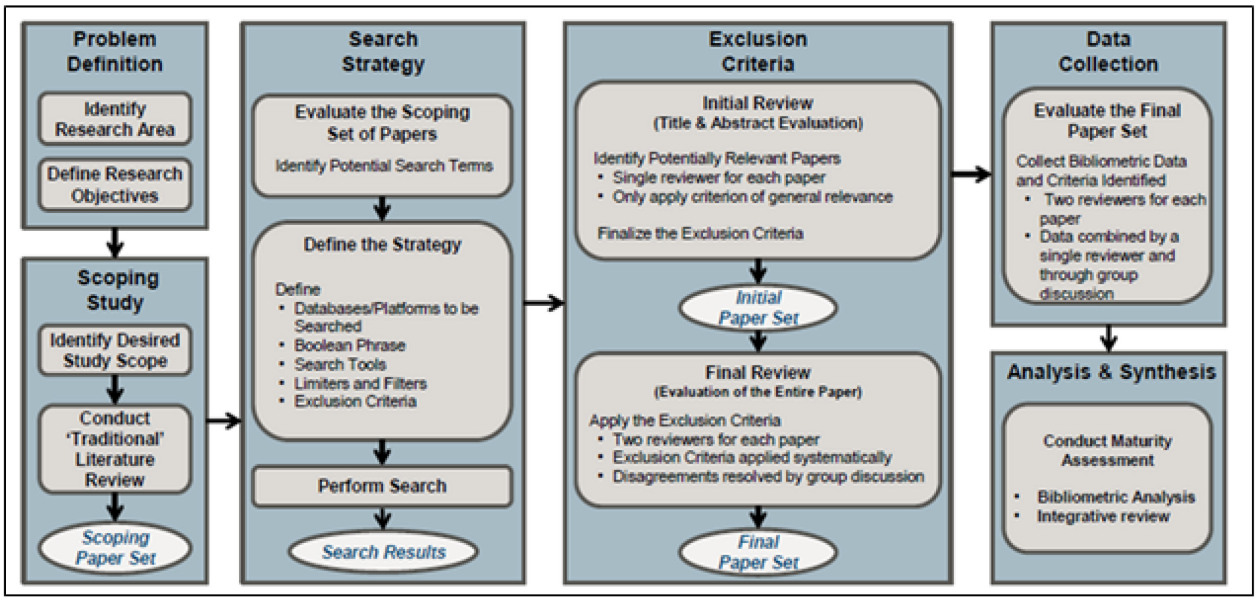

Figure 10-2: Systematic Literature Review Methodology.

Platform	Scopus	NATO library	SharePoint	Web of Science
Total number of results	14623	1991	/	10251
Number of papers retained	1600	46 (+45 doubles on Scopus)	99	1411
Number of documents retrieved	1177	46	99	1303
Number of missing documents	423	0	0	108

Previous Belgian contributions

Current contribution

Figure 10-3: Selection of Documents.

10.4.2 Data Analysis

An extraction tool was then built in MS Excel to extract the different types of data required to answer our research questions. This data included general bibliometric data such as the year of publication but also the different stakeholder groups mentioned within a paper, the different frameworks mentioned, the different countries of interest and the context the paper was referring too. As each paper was given a unique identification number, the different types of data were then matched via MS Excel processing sheets. The output of these processing sheets was then used to generate graphics and networks via NodeXL.

10.5 FINDINGS

10.5.1 What are the Main Strategic-Level Societal Stakeholder Groups Mentioned in the Literature?

A frequency count of the stakeholders mentioned within the paper set (Figure 10-4) gives us the following percentage of coverage for each stakeholder group: Government including federal departments and ministries (68% of papers), population (53%) and political stakeholders (46%) followed by partner countries (42%), international organisations (35%) and internal stakeholders (28%). While the prevalence of the first three stakeholder groups is not a surprise as such, this highlights the focus of existing research as well as the need for more research to better understand and further develop comprehensive and societal-level initiatives which equally focus on some of the stakeholder groups least mentioned. For example, only four papers out of the 206 papers focussed on first responders.

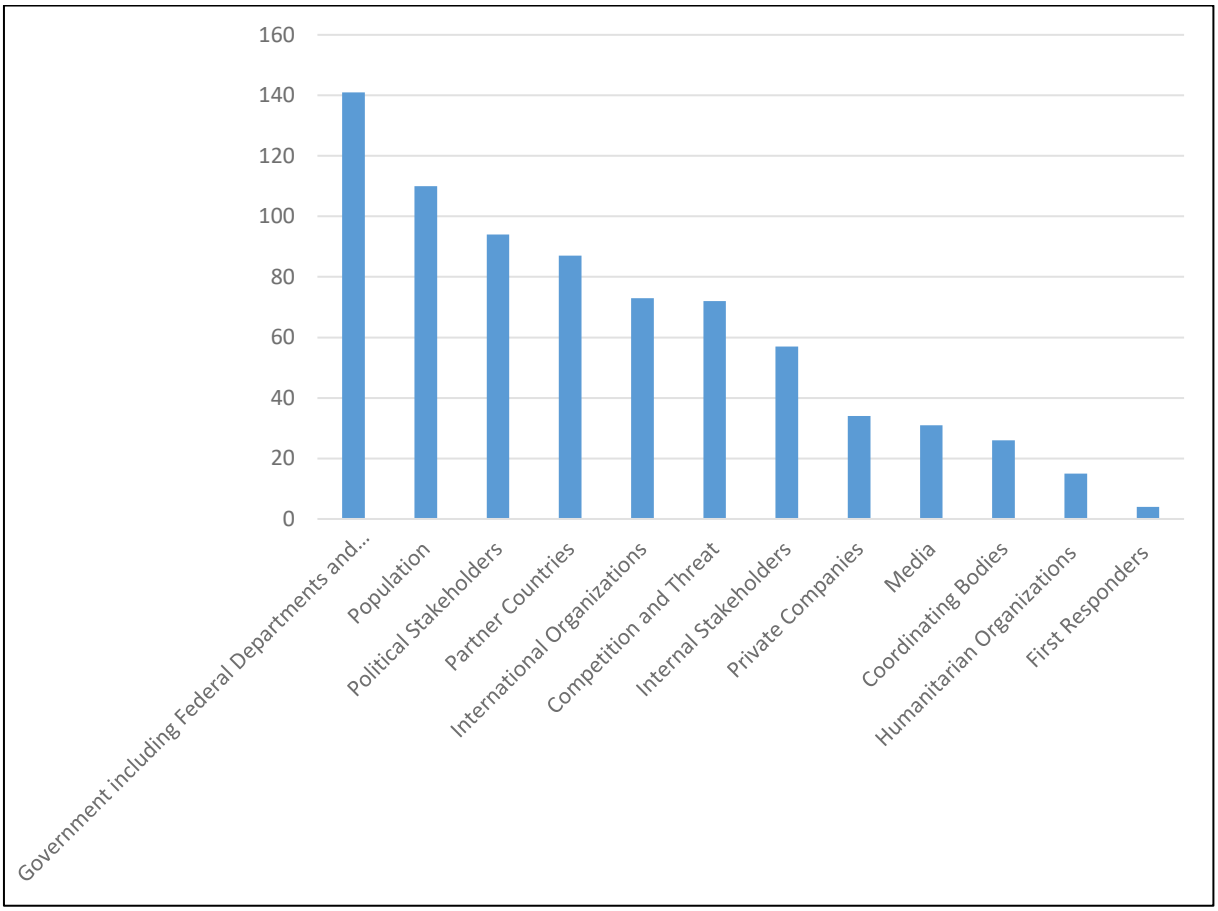

Figure 10-4: Stakeholders.

10.5.2 What are the Most Prevalent Frameworks Mentioned in the Literature?

The frequency count of frameworks mentioned within the paper set is as depicted in Figure 10-5. From the figure, several observations can be made. First, most papers delve on one stakeholder or the other without the consideration of a larger stakeholder network or stakeholder ecosystem as such. This seems coherent with previous observations that, despite the fact that defence organisations are said to be portraying increased attention to stakeholders, there is little empirical research reflecting the shift toward a holistic consideration of stakeholders by managers within the military [12]. Our second observation is that, while all defence organisations likely do crisis management and performance management in some form, not all these initiatives may be based on a structured approach. Third, some frameworks may find prominence due to their utilisation and promotion by NATO as in the case of the Means-Ways-Ends [22] and Host Nation Support. Other authors have described such a tendency of top-down pressure towards adoption of concepts in the field of comprehensive defence [14] and the NATO Defence Planning Process [45] in the past. Our fourth observation is that there is a gradual reflection in the empirical literature of the societal debate taking place regarding the new role for defence, where stakeholder management is much more complex than before. Amongst the frameworks used to structure this debate, it appears that Total Defence is the most studied concept. For a more detailed discussion on Total Defence, we refer to the Norwegian chapters.

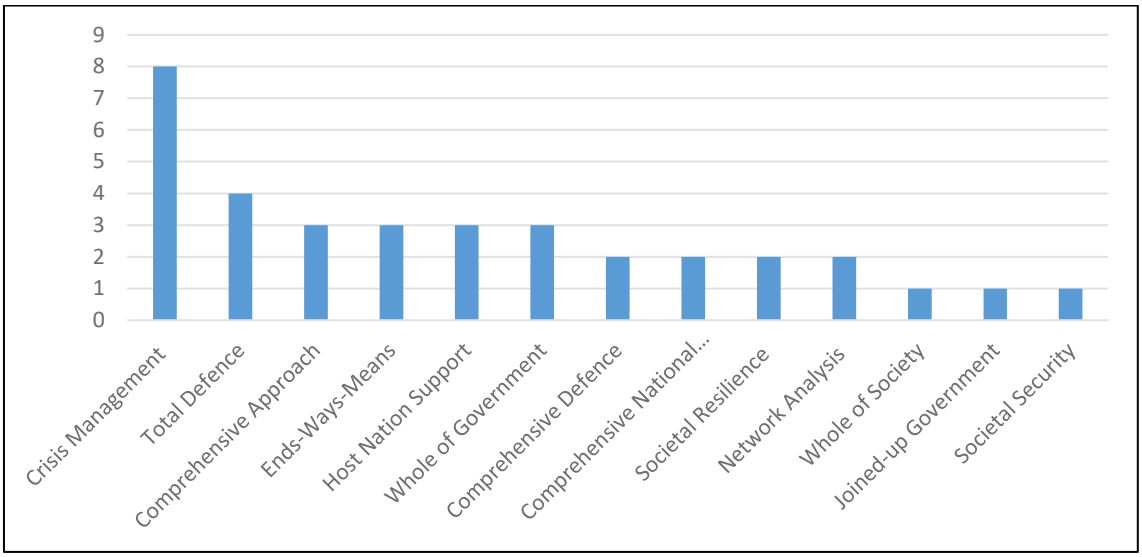

Figure 10-5: Frameworks.

Before analysing the distribution of the various frameworks over time, we have to mention that the seven papers received from the subject matter experts bore the time stamp of 2020 which impacts the results. However, even after accounting for this, we may be observing a gradual shift in the literature from the Means-Ways-Ends and Crisis Management frameworks towards the Comprehensive or 3D approach (Defence, Diplomacy and Development Aid) and lately the Societal resilience frameworks such as Total Defence. Therefore, when combining this observation with those originating from Figure 10-6, we can characterise comprehensive national defence systems as emergent. This reflects the change in landscape from conventional defence in the 1990s towards societal support and protection in the last decade. However, even if the subject is becoming more popular, the fact remains that this is a subject that is not often empirically studied and that a lot of expertise is currently based on non-empirical foundations.

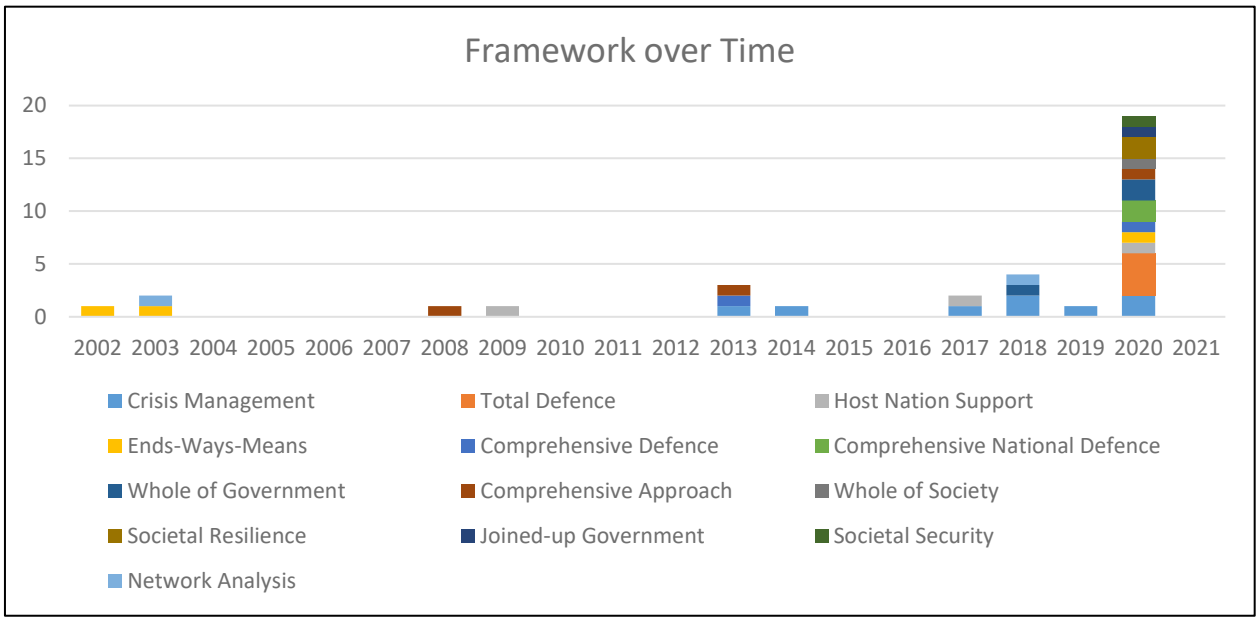

Figure 10-6: Framework Over Time.

Through our findings originating in Figure 10-5 and Figure 10-6, we also observe that no particular framework enjoys prominence, which can support claims of confusion when discussing comprehensive national defence initiatives. For example, Peets [45] claims that Estonian national defence initiatives have been selectively and differentially understood in different parts of the state system, which has made it difficult to harmonize cross-governmental initiatives. Accordingly, there may be a need for the use of a single framework including its set of underlying definitions, methodologies and doctrines within a given state.

10.5.3 How are the Most Prevalent Stakeholder Groups Linked to the Different Frameworks?

Figure 10-7 attempts to identify which stakeholder groups are mentioned simultaneously with the different frameworks previously referenced. For the purpose of clarity, we have attempted, in so far that this is possible, to order the national stakeholders on the right hand side, the international stakeholders on the left hand side, the internal stakeholders toward the bottom and the external stakeholders towards the top. Doing so allows us to identify three broad categories of frameworks, which is slightly different from our background literature study. The first category seems more 'traditional defence' focussed in so far as we identify defence stakeholder groups linked to legacy defence activities and the three following frameworks: Means-Ways-Ends, Host Nation Support and Crisis Management. The second category we identify is more 'Whole-of-Government' focussed in so far as it attempts to bring together a wider range of national stakeholders. Comprehensive Defence, Comprehensive Approach, Comprehensive National Defence, Whole-of-Government and Joined-up Government are part of this second category. Our third category is formed by the societal networks that probably depict less linkages with stakeholder groups at this time due to their emergent nature. Again, one exception seems to be Total Defence that, besides being the most prevalent after crisis management as previously stated, also depicts the highest amount of linkages with the different stakeholder groups along with Whole-of-Government.

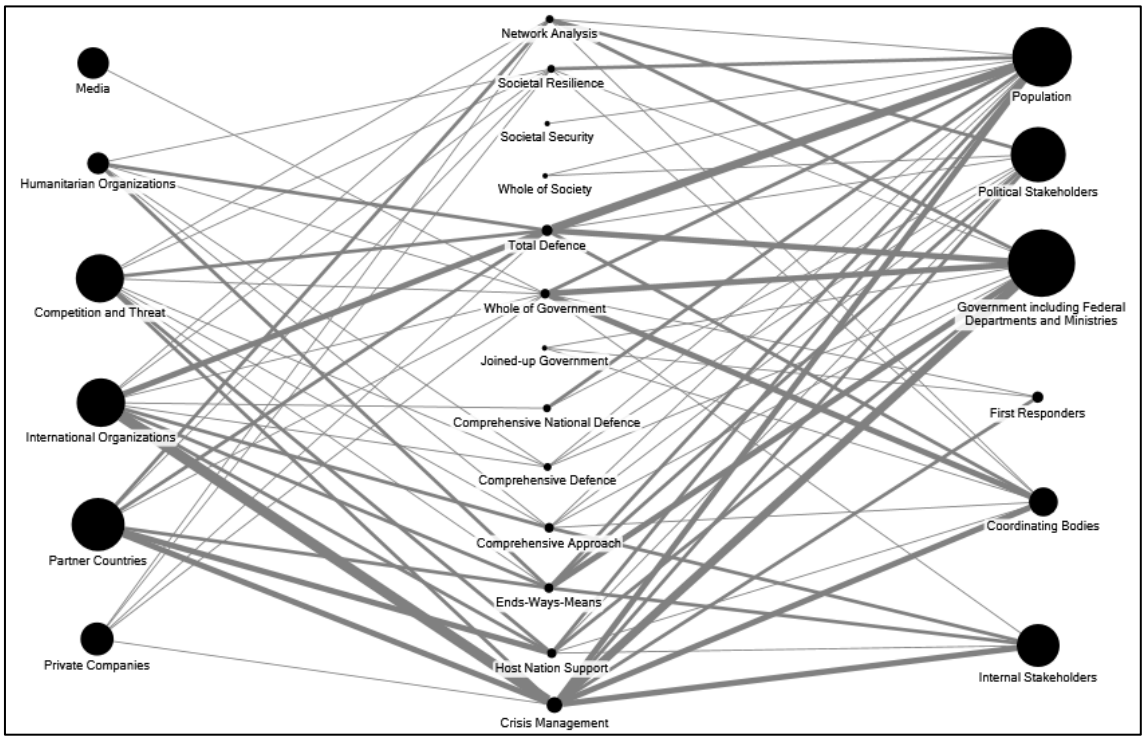

Figure 10-7: Frameworks versus Stakeholders

10.5.4 What are the Factors that Influence the Stakeholders Network?

In order to answer research question three, we first had to select which relevant aspects and factors we had to explore. The first aspect we identified was 'performance management' as the literature seemed to indicate the existence of a link between the performance of an organisation and its stakeholder network [24], [44], [10]. For example, Van Bockhaven, Matthyssens and Vandenbempt [55] mention network volume as a structural performance determinant. In Figure 10-8, we establish the link between the country being analysed within a paper and any stakeholder group being mentioned within the context of the same paper. For this purpose, we clustered the nations based on their performance management maturity level which we retrieved from a previous NATO study delving on performance management in defence organisations [22]. Unfortunately, not all countries participated in the said study whereby we were only able to meaningfully depict a total of 13 countries in our figure. Our main observation is that the countries with the highest maturity levels (US[1] and UK) seemed to be linked to all stakeholder groups. Also, the stakeholder groups least studied are the same as the ones previously identified (coordinating bodies, first responders, the media, and humanitarian organisations), but this may be more exacerbated in the case of countries identified as having a lower performance management maturity level.

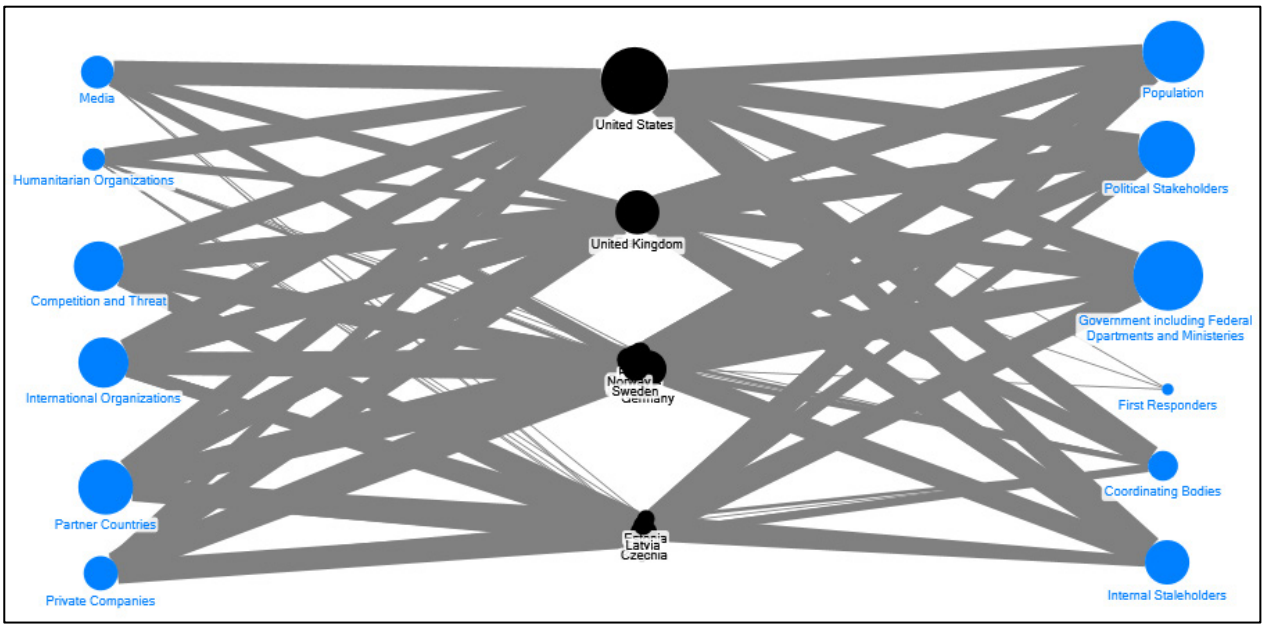

Figure 10-8: Country vs. Stakeholders NATO Cluster.

The second factor we explored versus the stakeholder group network was armed force type, which is a reflection of the ambition level of a country's armed forces [22]. The reason we retained armed force type is the fact that it was the factor that seemed to have the highest correlation with the performance management maturity level in the previous NATO study. While a clustering of NATO and EU nations according to their armed force type was not readily identified, we were inspired by the IISS capability matrix [23] which resulted in the clustering depicted in Figure 10-9[2]. This figure also depicts the USA and UK being mentioned along with all stakeholder groups (12) followed by France, Germany, and Italy (11). Again, the last cluster (representing the countries with lesser military ambition) seems to be less frequently analysed along with stakeholder groups such as the media and humanitarian organisations. The results are therefore similar to the previous findings regarding the performance maturity level. The proposition follows that more ambitious

[1] The USA did not participate in the NATO study, but its maturity level was assessed based on available evidence in the literature.

[2] The same figure excluding US data to improve readability can be found in Appendix 10.1.

armed forces, which likely make greater use of performance measurement/management techniques, may be better placed to leverage their stakeholder network.

The third factor we explored with respect to the stakeholder groups was the context within which they were being discussed. We established the different contexts according to the level of violence, broadly in line with the concept of escalation as is discussed by Murumets [38] and Endregard [19]. In total we recorded 130 papers investigating peacetime, 92 on crisis, 105 on missions or operations and 119 on wartime. As we have a total of 206 papers analysed in our final paper set, these numbers reflect the VUCA[3] environment in so far as authors loosely discuss several different contexts within a single paper. While this reflects the contemporary environment, it likely makes it more difficult for researchers to determine the boundaries of their studies and results.

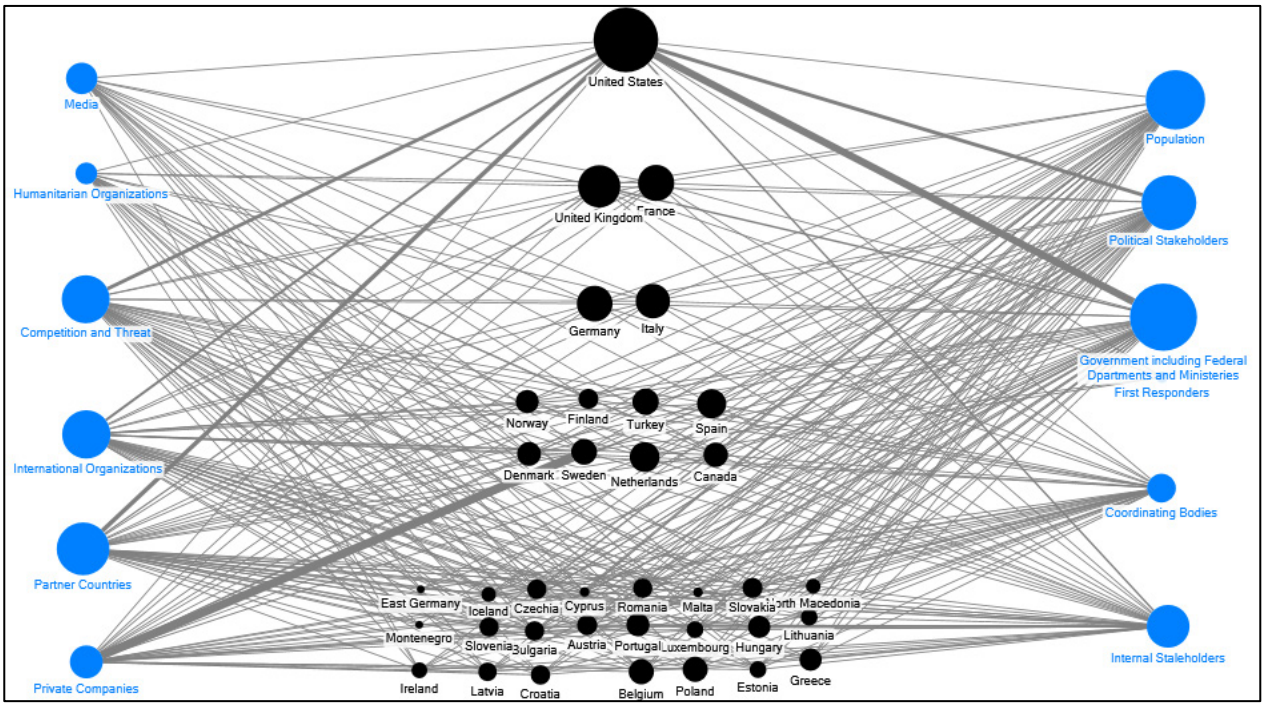

Figure 10-9: Country vs. Explanatory Factor (Armed Force Type) vs. Stakeholders.

In Table 10-2, we matched the stakeholder groups to the different contexts mentioned within a paper and further scaled the stakeholder group numbers based on the context count. In doing so, we observe stakeholder groups that are important across all contexts such as the Government including federal departments and ministries, followed by the political stakeholders and the population. We also identified stakeholder groups that are under leveraged across all contexts, such as coordinating bodies, private companies, humanitarian organisations, the media and first responders (who enjoy the least amount of attention across all contexts). Our third observation is that the ranking of the stakeholder groups seems similar in peace time (Government including federal departments and ministries, partner countries, political stakeholders followed by the population) and war time (Government including federal departments and ministries, population, political stakeholders followed by partner countries) even if the intensity of stakeholder engagement seems to be higher in peace time, as the situation may perhaps permit this. In war time, there may be relatively more focus on the important stakeholder groups being the Government including federal departments and ministries and the population. Our fourth observation is that, in war time as well as in missions and operations, there may be two main steering mechanisms taking place which need

[3] Volatile Uncertain Complex and Ambiguous.

to be synchronised, being the national steering process (with a focus on the Government including federal departments and ministries, the population and political stakeholders) and the international steering process (with the focus being on partner countries and international organisations). Our last observation is that private companies may be more the focus of attention in peace time, which is perhaps linked to the fact that a limited number of countries engage actively and massively with private companies in more kinetic contexts.

In Figure 10-10 we transposed the results of the table into a network structure similarly to the previous attempts to differentiate the different stakeholder groups along an international versus national axis and an internal versus an external axis. In addition, we also coded and depicted as a context the papers that discuss terrorism. While the results broadly reflect those of the Table 10-2, we observe that the Government including federal departments and ministries as a stakeholder group is slightly surpassed by the population within the context of terrorism.

Table 10-2: Stakeholder by Context – Scaled.

	Peace	Crisis	Mission Operation	War
Count	130	92	105	119
%	0.264766	0.187373	0.213849	0.242363
Internal Stakeholders	10,33	3,75	7,70	8,00
Government including Federal Departments and Ministries	22,77	11,80	18,39	21,81
First Responders	0,53	0,75	0,43	0,24
Coordinating Bodies	5,56	2,06	2,99	3,39
Political Stakeholders	16,42	6,18	13,69	13,81
Population	15,89	8,24	14,54	18,90
Partner Countries	17,21	7,68	10,91	11,88
International Organizations	12,71	5,81	9,41	9,21
Private Companies	7,94	1,50	2,35	2,42
Humanitarian Organizations	1,85	1,50	2,35	1,94
Media	5,56	2,62	4,06	5,09
Competition and Threat	12,44	5,43	9,84	11,39

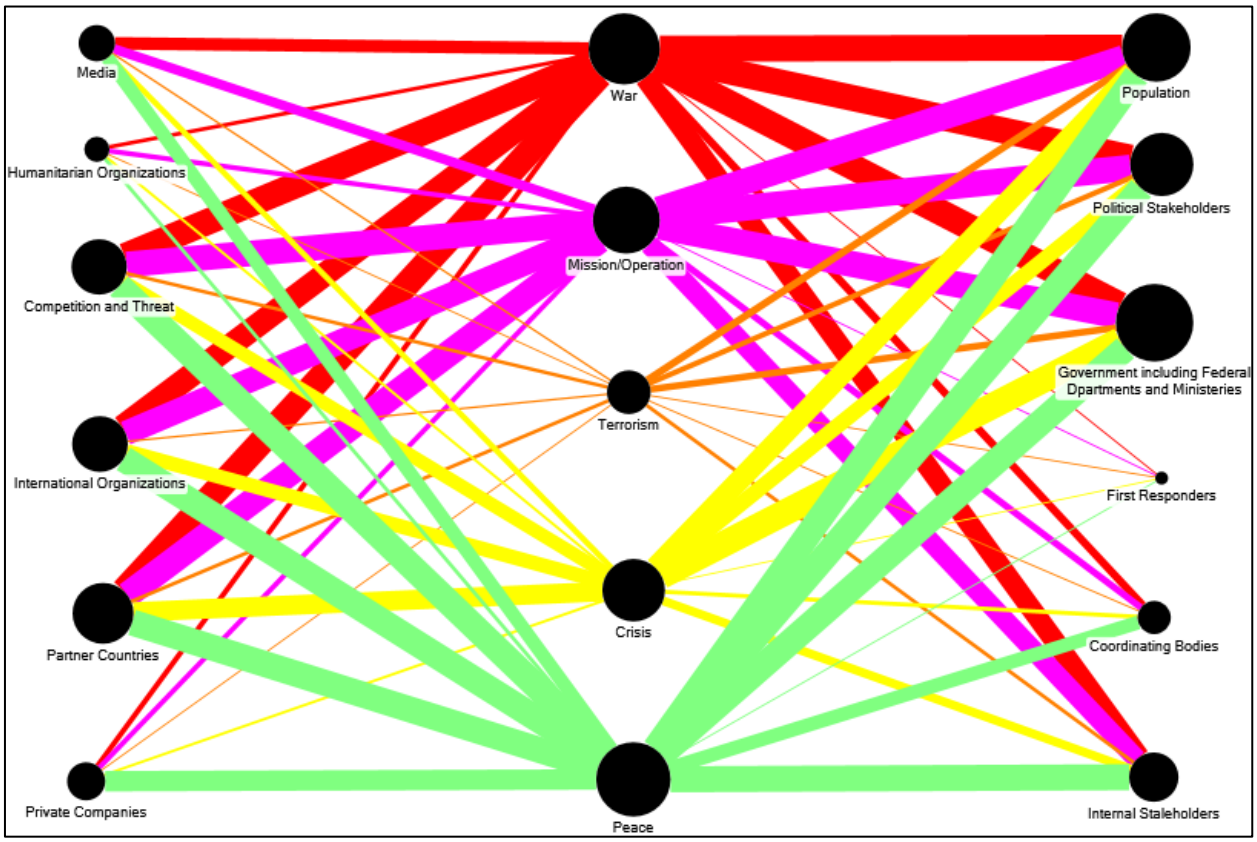

Figure 10-10: Stakeholder by Context – Scaled.

10.6 DISCUSSION AND MANAGERIAL IMPLICATIONS

Our findings indicate that there may be room for defence organisations, especially those that are characterised by a lower performance maturity level, to expand their stakeholder network. This can be linked to activities taking place within comprehensive national defence and its emergence into societal-level initiatives. However, the question as to how managers should proceed in enlarging the organisation's stakeholder network and whether this would translate into organisational benefits still remains to be answered. It seems reasonable to state that armed force type or the ambition level is not changeable overnight if at all, and that increasing the organisation's performance maturity level is a long-term change management effort. While the literature does establish a link between the performance of an organisation and its stakeholder network [24], [44], [10], it also makes clear that enhanced stakeholder management imposes coordination challenges and costs [45] while requiring organisational abilities such as sense making, framing, strategic communication and risk assessment [5], [49], [19]. According to the last author, risk assessment alone implies a large variety of competencies and knowledge, both within and outside the organisation. In this light, Maitlis and Sonenshein [33] state that there needs to be a balance between the ability of an organisation to process stakeholder complexity from within with respect to the "danger" of introducing even more complexity than can be handled. While the authors call for additional research on how organisations handle this trade-off, other authors have made the case that too much focus on stakeholder engagement itself is detrimental to organisation performance [26]. There may therefore be a need for a progressive build-up of the organisational stakeholder engagement capability preceding or accompanying consequential expansion in the stakeholder network linked to societal framework implementation efforts.

10.7 CONCLUSION

Our study set out to explore how the different stakeholders of NATO and EU defence organisations as well as the different comprehensive national defence frameworks were being discussed in the literature. As we exploited the results of an available systematic literature review [29] and based our findings on a unique set of 199 empirical papers, we addressed a research gap which is the dearth of evidence-based insights characterising the field [18], [12].

After initially proposing a taxonomy dividing the most important stakeholders into stakeholder groups, we identified those stakeholder groups that were more (such as the Government including federal departments and ministries, discussed in 68% of the papers) or less prominent (such as first responders, discussed in less than 2% of the papers). Thereafter, we established that amongst the different frameworks being discussed, Total Defence [60] was the most studied framework while also exhibiting the highest number of linkages with the different stakeholder groups. This highlights the holistic nature of Total Defence and its possible emergence as a baseline for future comprehensive national defence initiatives. Further, while exploring some of the factors influencing the stakeholder network of defence organisations (such as the performance maturity level of the organisation, the country, and the armed force type), we were able to identify countries that are likely more advanced in the field with respect to others. We proposed that more ambitious armed forces that make greater use of performance measurement and management techniques may be better placed to leverage their stakeholder network. At the same time, we proposed that other defence organisations wanting to expand their stakeholder network have to synchronise this ambition with their own internal stakeholder engagement capability.

On a more generic level, our literature study supports some of the trends discussed in other chapters of this report, such as an enlargement in focus from an international perspective to a national perspective on stakeholders, an increase in the number of stakeholders being studied per manuscript over time (which indicates that studies are accounting for a more holistic approach) and an increase in manuscripts discussing several contexts simultaneously (which is a testimony of the current VUCA environment). Taken together, these trends imply a paradigm shift for defence organisations from a situation where they were able to fully impact the environment pertaining to traditional defence matters, towards a situation where a constant attempt has to be made to influence and contribute to society.

10.8 FUTURE RESEARCH

While our study established that comprehensive national defence frameworks were likely becoming increasingly ‘comprehensive’, the fact is that they are just not studied often empirically. This substantiates Egnell’s [18] findings that the conceptual and doctrinal developments underpinning the field are based on weak historical, theoretical, and qualitative assumptions instead of solid empirical data. According to the author, this implies that causal relationships between cooperation and effectiveness in the field of defence, security and development still need to be established.

One avenue for future research is a more detailed cartography of strategic-level defence stakeholders beyond the large ‘bucket’ of stakeholder groups employed within this study. A subsequent topic of interest is a deeper study of the ‘power – interest’ profile of these different stakeholders as is often studied in other domains. For example, one could compare the stakeholder profiles and the existing command and control mechanisms to the SAS085 C2 maturity model [39]. In turn, this should support the development of more tailored (and possibly more effective) stakeholder and societal engagement strategies, raise the level of internal comprehensive defence awareness, and kick-off normative debate on topics such as cultural homogeneity and requisite variety.

10.9 ACKNOWLEDGEMENT

First, we would like to thank Yaroslav Spichak, Sofia Flores, Juan Villalobos and Diego Tovar-Lopenza of the University of Central Florida who took part in the initial review of the SLR process. As this ultimately facilitated the generation of some of the insights presented in this chapter, their contribution is invaluable. Second, we would also like to acknowledge the guidance, comments and feedback received from Professor Heather Keathley-Herring from the Industrial Engineering and Management Systems Department of the University of Central Florida. Last, we acknowledge funding from the Royal Higher Institute for Defence (Brussels).

10.10 REFERENCES

[1] Andres, M. (2015), "Werkrelaties tussen militairen en burgerpersoneel bij Defensie", Militaire Spectator : Tijdschrift voor het Nederlandsche leger, 184(9), pp. 374-387.

[2] Apte, A., Gonçalves, P. and Yoho, K. (2016), "Capabilities and competencies in humanitarian operations", Journal of Humanitarian Logistics and Supply Chain Management, 6(2), pp. 240-258. doi: 10.1108/JHLSCM-04-2015-0020.

[3] Archuleta, B.J. (2016), "Rediscovering defense policy: A public policy call to arms", Policy Studies Journal, 44, pp. S50-S69. doi: 10.1111/psj.12157.

[4] Arsenault, E.G. and Chiang, C. (2020), "The U.S. Department of Defense and its torture program", Armed Forces and Society, 46(2), pp. 191-213. doi: 10.1177/0095327X19840067.

[5] Arslan, E. (2022), "Comprehensive defence for city security", NATO Science and Technology Organisation, Paris.

[6] Balcaen, P., Du Bois, C. and Buts, C. (2021), "A game-theoretic analysis of hybrid threats", Defence and Peace Economics, 33(1), pp. 26-41. doi: 10.1080/10242694.2021.1875289.

[7] Berndtsson, J. (2019) "The market and the military profession: Competition and change in the case of Sweden", Defense and Security Analysis, 35(2), pp. 190-210. doi: 10.1080/14751798.2019.1600798.

[8] Berzina, I. (2022), "Cognitive dimension of comprehensive national defence", NATO Science and Technology Organisation, Paris.

[9] Boylan, S. (2015), "Public opinion", Military Review, (September-October), pp. 93-105. doi: 10.3917/soc.100.0007.

[10] Briones-Peñalver, A.J., Bernal-Conesa, J.A. and de Nieves Nieto, C. (2020), "Knowledge and innovation management model: Its influence on technology transfer and performance in Spanish defence industry", International Entrepreneurship and Management Journal, 16(2), pp. 595-615. doi: 10.1007/s11365-019-00577-6.

[11] Caprioli, M. and Trumbore, P.F. (2005), "Rhetoric versus reality: Rogue states in interstate conflict", Journal of Conflict Resolution, 49(5), pp. 770-791. doi: 10.1177/0022002705279335.

[12] Chinta, R., Hagan, M.F. and Sussan, F. (2015), "Stakeholder considerations and action orientation among managers in the military", Journal of Military and Information Science, 3(1), pp. 4-12.

[13] Corbetta, R. and Dixon, W. (2004), "Multilateralism, major powers, and militarized disputes", Political Research Quarterly, 57(1), pp. 5-14.

[14] De Craene, C. (2018), "Het concept 'fragiliteit' bij de planning en uitvoering van Belgische militaire operaties in het kader van een interdepartementale samenwerking", Royal Military Academy, Brussels.

[15] Daems, I. (2014), "Pre-, during, and post-deployment psychological care for soldiers and their families in the Austrian and Belgian Armed Forces", Royal Military Academy, Brussels.

[16] Dillon, R.L., Liebe, R.M. and Bestafka, T. (2009), "Risk-based decision making for terrorism applications", Risk Analysis, 29(3), pp. 321-335. doi: 10.1111/j.1539-6924.2008.01196.x.

[17] Egnell, R. (2006), "Explaining US and British performance in complex expeditionary operations: The civil-military dimension", Journal of Strategic Studies, 29(6), pp. 1041-1075. doi: 10.1080/01402390601016717.

[18] Egnell, R. (2013), "Civil-military coordination for operational effectiveness: Towards a measured approach", Small Wars and Insurgencies, 24(2), pp. 237-256. doi: 10.1080/09592318.2013.778017.

[19] Endregard, M. (2022), "Challenges of a risk-based approach to national security for a digitised total defence", NATO Science and Technology Organisation, Paris.

[20] Endres, F., Mader, M. and Schoen, H. (2015), "On the relationship between strategic cultures and support for European defence: A comment on Irondelle, Mérand and Foucault", European Journal of Political Research, 54(4), pp. 848-859. doi: 10.1111/1475-6765.12109.

[21] Freeman, R.E. (1994), "The politics of stakeholder theory: Some future directions", Business Ethics Quarterly, 4(4), pp. 409-421.

[22] NATO STO (2020), "Performance management in defence organisations", STO-TR-SAS-096-Part-I, NATO Science and Technology Organization, Neuilly-sur-Seine, France.

[23] Giegerich, B., Childs, N. and Hackett, J. (2018), "Military capability and international status", Military Balance blog, Available at: https://www.iiss.org/blogs/military-balance/2018/07/military-capability-and-international-status (Accessed: 11 June 2022).

[24] Goerzen, A. and Beamish, P.W. (2005), "The effect of alliance network diversity on multinational enterprise performance", Strategic Management Journal, 26(4), pp. 333-354. doi: 10.1002/smj.447.

[25] Grunnan, T., Endregard, M., Siedler, R.E., and Elstad, A-K. (2020), "Norwegian societal security and state security – challenges and dilemmas", in Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference, pp. 4596-4603. doi: 10.3850/978-981-14-8593-0_4467-cd.

[26] Hardy, C., Lawrence, T. B. and Phillips, N. (2006), "Swimming with sharks: Creating strategic change through multi-sector collaboration", International Journal of Strategic Change Management, 1(1/2), pp. 96-112. doi: 10.1504/ijscm.2006.011105.

[27] Hiebert, R. E. (2003), "Public relations and propaganda in framing the Iraq war: A preliminary review", Public Relations Review, 29(3), pp. 243-255. doi: 10.1016/S0363-8111(03)00047-X.

[28] Karlsrud, J. (2015), "The UN at war: Examining the consequences of peace-enforcement mandates for the UN peacekeeping operations in the CAR, the DRC and Mali", Third World Quarterly, 36(1), pp. 40-54. doi: 10.1080/01436597.2015.976016.

[29] Keathley, H. (2016) "The systematic literature review process", University of Central Florida, Orlando.

[30] Kiszely, J. (2019) "The political-military dynamic in the conduct of strategy", Journal of Strategic Studies, 42(2), pp. 235-258. doi: 10.1080/01402390.2018.1497488.

[31] L'Eveque, G. (2017) "Defence, diplomacy and development, de Belgische 3D benadering", Royal Military Academy, Brussels.

[32] Lonsdale, D. (2016), "Britain's emerging cyber-strategy", The RUSI Journal, 161(4), pp. 52-62.

[33] Maitlis, S. and Sonenshein, S. (2010), "Sensemaking in crisis and change: Inspiration and insights from Weick (1988)", Journal of Management Studies, 47(3), pp. 551-580. doi: 10.1111/j.1467-6486.2010.00908.x.

[34] Malešič, M. (2015), "The impact of military engagement in disaster management on civil-military relations", Current Sociology, 63(7), pp. 980-998. doi: 10.1177/0011392115577839.

[35] Maxey, S. (2021), "Limited spin: When the public punishes leaders who lie about military action", Journal of Conflict Resolution, 65(2-3), pp. 283-312. doi: 10.1177/0022002720961517.

[36] Møller, J. E. (2019), "Trilateral defence cooperation in the North: An assessment of interoperability between Norway, Sweden and Finland", Defence Studies, 19(3), pp. 235-256. doi: 10.1080/14702436.2019.1634473.

[37] Mousseau, M. (2009), "The social market roots of democratic peace", International Security, 33(4), pp. 52-86.

[38] Murumets, J. (2007), "Concept of escalation", in Proceedings of the Estonian National Defense College 7/2007, pp. 148-149.

[39] Murumets, J. and Ermus, A. (2023), "Concept model of combined headquarters", Chapter 16 in "Conceptual Framework for Comprehensive National Defence System", NATO STO Technical Report STO-TR-SAS-152, NATO Science and Technology Organization, Neuilly-sur-Seine, France.

[40] Norri-Sederholm, T., Norvanto, E., Talvitie-Lamberg, K., Huhtinen, A-M. (2015), "Social media as the pulse of national security threats: A framework for studying how social media influences young people's safety and security situation picture", International Journal of Special Education, 30(2), pp. 70-84.

[41] Org, L. (2022), "Legal aspects of integrating Armed Forces into internal security tasks", Chapter 15 in "Conceptual Framework for Comprehensive National Defence System", NATO STO Technical Report STO-TR-SAS-152, NATO Science and Technology Organization, Neuilly-sur-Seine, France.

[42] Otzulis, V. and Ozolina, Ž. (2017) "Shaping Baltic States defence strategy: Host nation support", Lithuanian Annual Strategic Review, 15(1), pp. 77-98. doi: 10.1515/lasr-2017-0004.

[43] Parrein, P-J. (2009) "De evolutie en toekomst van de Belgisch-Nederlandse marinesamenwerking: Spill-over en politieke samenwerking", Royal Higher Institute for Defence, Brussels.

[44] Pedrini, M. and Ferri, L.M. (2019), "Stakeholder management: A systematic literature review", Corporate Governance", 19(1), pp. 44-59. doi: 10.1108/CG-08-2017-0172.

[45] Peets, I. (2022), "Enterprise architecture and capability-based planning: Tools for efficient State", Chapter 13 in "Conceptual Framework for Comprehensive National Defence System", NATO STO Technical Report STO-TR-SAS-152, NATO Science and Technology Organization, Neuilly-sur-Seine, France.

[46] Plowman, K.D. (2013), "Creating a model to measure relationships: U.S. Army strategic communication", Public Relations Review, 39(5), pp. 549-557. doi: 10.1016/j.pubrev.2013.07.001.

[47] Sauer, T. (2015), "Deep cooperation by Belgian defence: Absorbing the impact of declining defence budgets on national capabilities", Defence Studies, 15(1), pp. 46-62. doi: 10.1080/14702436. 2015.1005900.

[48] Saxi, H.L. (2017), "British and German initiatives for defence cooperation: The Joint Expeditionary Force and the Framework Nations Concept", Defence Studies, 17(2), pp. 171-197. doi: 10.1080/ 14702436.2017.1307690.

[49] Seidl, D. and Werle, F. (2018) "Inter-organizational sensemaking in the face of strategic meta-problems: Requisite variety and dynamics of participation", Strategic Management Journal, 39(3), pp. 830-858. doi: 10.1002/smj.2723.

[50] Shambaugh, G., Matthew, R.A., Silver, R.C., McDonald, B., Poulin, M., and Blum, S. (2010), "Public perceptions of traumatic events and policy preferences during the George W. Bush administration: A portrait of America in turbulent times", Studies in Conflict and Terrorism, 33(1), pp. 55-91. doi: 10.1080/10576100903488410.

[51] Soares, J., Verburg, M. and Letens, G. (2020), "The Comprehensive approach in Belgium: The state of affairs in 2020 based on a case study of the Belgian Defence", Chapter 3 in NATO STO (2021), "Conceptual framework for comprehensive national defence system", Interim report of the SAS-152 study: Review of literature, case studies and preliminary findings. NATO STO Technical Report STO-TR-SAS-152-Part-I. Pre-release. NATO STO, Neuilly-sur-Seine, France.

[52] Thompson, G. and Louth, J. (2019), "Understanding transparency in UK defence management", Financial Accountability and Management, 35(3), pp. 246-257. doi: 10.1111/faam.12194.

[53] Thomson, C.P. and Blagden, D. (2018), "A very British national security state: Formal and informal institutions in the design of UK security policy", British Journal of Politics and International Relations, 20(3), pp. 573-593. doi: 10.1177/1369148118784722.

[54] Ušiak, J. (2018), "Security-related cooperation among the V4 States", Politics in Central Europe, 14(2), pp. 39-56. doi: 10.2478/pce-2018-0008.

[55] Van Bockhaven, W., Matthyssens, P. and Vandenbempt, K. (2015), "Drivers of institutional innovation in networks: Unleashing the innovation potential of domesticated markets", Journal of Business & Industrial Marketing, 30(3/4), pp.414-435.

[56] Wallenius, C., Brandow, C., Berglund, A.K., and Jonsson, E. (2019), "Anchoring Sweden's post-conscript military: Insights from elites in the political and military realm", Armed Forces and Society, 45(3), pp. 452-471. doi: 10.1177/0095327X18755107.

[57] Wither, J.K. (2020), "Back to the future? Nordic total defence concepts", Defence Studies, 20(1), pp. 61-81. doi: 10.1080/14702436.2020.1718498.

[58] Ybarra, C., Bueno, I., Endregard, M., Blatny, J.M., Dugauquier, C., Dhermain, J., Petronio, G., Engman, L.K. (2009), "Counter biological and chemical terrorism WP6000: Emergency preparedness and response", Norwegian Defence Research Establishment.

[59] Yilmaz, S. (2022), "Adaptation of emerging technologies into Defence", NATO Science and Technology Organization, Neuilly-sur-Seine, France.

[60] Zdanavičius, L. and Statkus, N. (2020), "Strengthening resilience of Lithuania in an era of Great Power competition: The case for total defence', Journal on Baltic Security, 6(2), pp. 1-21. doi: 10.2478/jobs-2020-0009.

Appendix 10-1: ADDITIONAL STAKEHOLDER INFORMATION

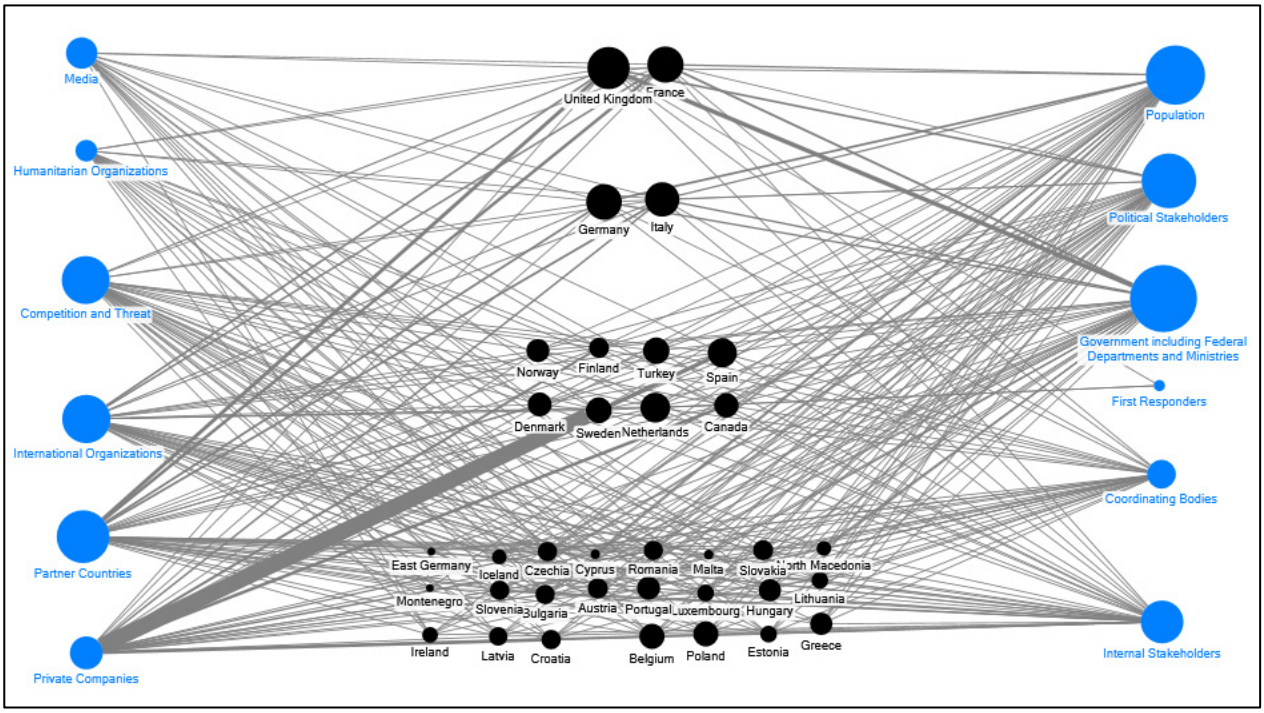

Figure 10A1-1: Country vs. Explanatory Factor (Armed Force Type) vs. Stakeholders

Table 10A1-1: Stakeholder by Context.

	Peace	Crisis	Mission Operation	War
Internal Stakeholders	39	20	36	33
Government including Federal Departments and Ministries	86	63	86	90
First Responders	2	4	2	1
Coordinating Bodies	21	11	14	14
Political Stakeholders	62	33	64	57
Population	60	44	68	78
Partner Countries	65	41	51	49
International Organizations	48	31	44	38
Private Companies	30	8	11	10
Humanitarian Organizations	7	8	11	8
Media	21	14	19	21
Competition and Threat	47	29	46	47

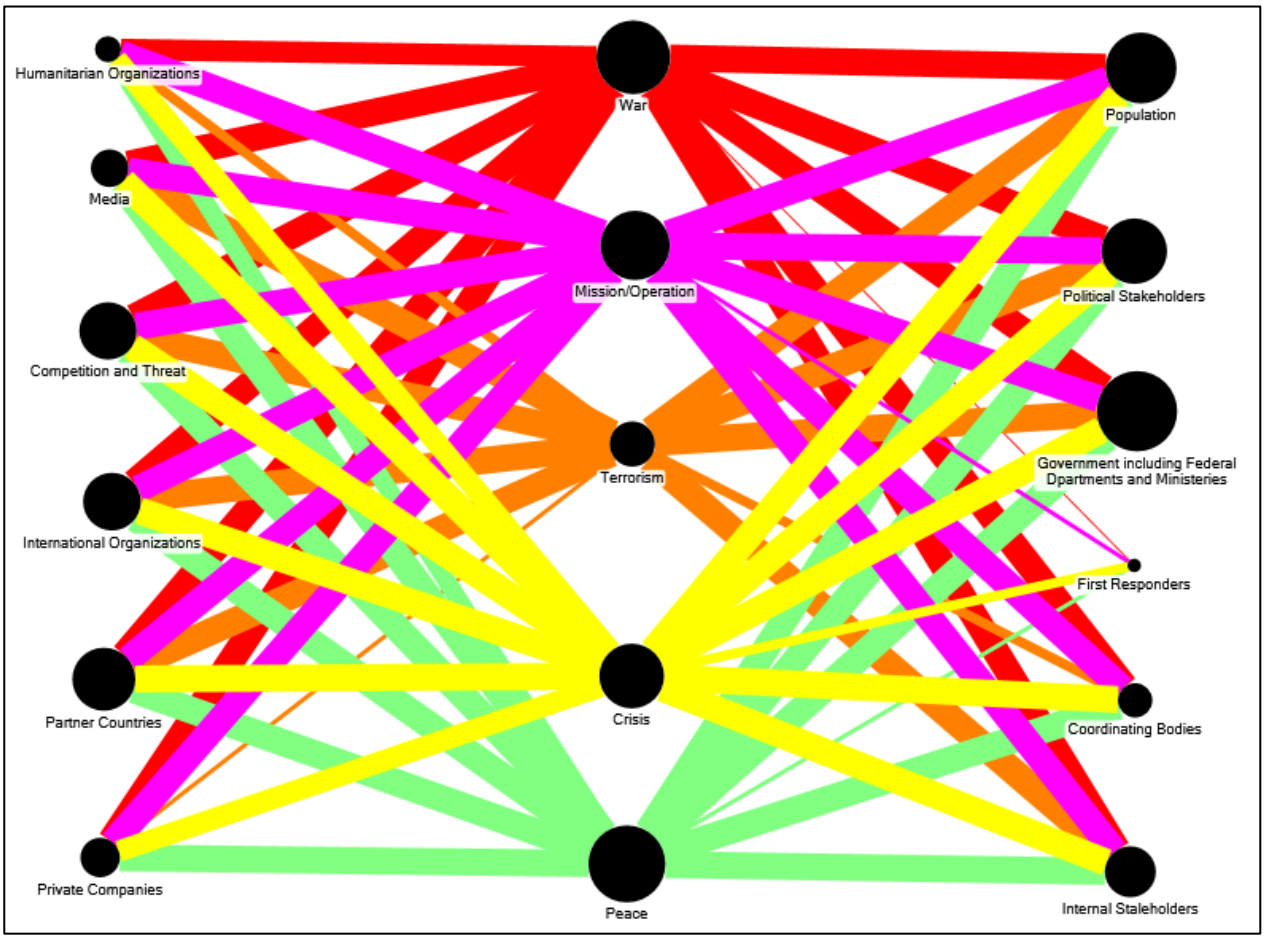

Figure 10A1-2: Stakeholder by Context.

Chapter 11 – COGNITIVE DIMENSION OF COMPREHENSIVE NATIONAL DEFENCE

Ieva Berzina
National Defence Academy of Latvia
LATVIA

The chapter describes the cognitive dimension of comprehensive national defence, which relates to competencies, views, and attitude required for this security concept at individual, organisational and societal levels. It builds on the premise that comprehensive national defence's ultimate aim is the resilience of a state and society to any crisis and an ability to resist the military and non-military aggression. The chapter addresses the research question: what are cognitive preconditions for resilience and resistance at a societal level? The research question is being answered by explaining the role of information-related processes in 21st-century warfare, the cognitive aspects of the information environment, public opinion as a domain of warfare, and the cognitive elements of resilience and resistance.

11.1 INTRODUCTION

An intrinsic element of warfare has always been intangible aspects such as morale, views and attitudes, perceptions, and others. History knows countless examples of when a warring party could achieve political and military goals more effectively or solely by manipulating the human mind. Issues related to information flows and their impact on political and military decision makers, domestic and overseas audiences are even more essential during the information age. The U.S. Marine Air Ground Task Force (MAGTF) Information Environment Operations Concept of Employment recognises that "the IE [information environment] is a key component of the commander's assigned operational environment and battlespace" (Ref. [89], p. 22). At the same time, the information dimension of warfare is a broad and complex phenomenon, which includes both technological and cognitive aspects. American Psychological Association defines cognition as "all forms of knowing and awareness, such as perceiving, conceiving, remembering, reasoning, judging, imagining, and problem solving. Along with affect and conation, it is one of the three traditionally identified components of mind" [4]. The cognitive dimension of warfare manifest primarily in the influence of human mind at individual, organisational, and societal level.

The cognitive aspects are an integral part of the information-related processes because personal and public views, attitudes, and behaviour form due to the information people are exposed to. The rapid development of information and communication technologies (ICT) since the 1990s determines the growing impact of information on international and national security. During the last three decades, global and regional powers and international organisations have developed numerous information-related policies and doctrines in the sphere of international and national security. These documents describe various concepts and ideas such as information security, information operations, information warfare, information environment, information battlefield, cyberspace, information superiority, strategic communication, psychological operations, disinformation, and others. Actors of international relations use these instruments to affect and protect the cognitive processes of specific target groups and domestic, overseas, and global audiences in general. The focus of the chapter is the effects of activities in the information environment at a societal level which manifest as public opinion. The interest in public opinion as a lever of power in international relations and national defence is determined by the growing importance of the ICT on a global scale, which increases the role of public opinion in political and military processes. At the same time, public opinion can be purposefully influenced and shaped, making it a powerful non-military instrument to achieve political and military goals.

The chapter conceptualises the role of public opinion within the comprehensive national defence. It is a specific defence strategy based on the whole-of-government approach and whole-of-society involvement principles. These principles imply that national defence exceeds the boundaries of military defence, because the characteristic feature of 21st-century warfare is the increasing use of non-military means to achieve political and military goals. Thus, all domains of social life being under the governance of different ministries should operate in a coordinated manner to reduce vulnerabilities, increase resilience, and resist malign foreign influence and aggression. It also means that national defence is the obligation of every individual, starting from crisis preparedness and ending with involvement in military defence. The effectiveness of comprehensive national defence depends on the ability to mobilise the whole population for national defence; therefore, it largely depends on public views, attitudes, and behaviour concerning national defence. The importance of public opinion also determines that cognitive dimension is a target of malign foreign influence aimed to demoralise society and promote a worldview favourable to the aims of an adversary.

11.2 THE COGNITIVE DIMENSION OF THE INFORMATION ENVIRONMENT

The cognitive aspects of comprehensive national defence should be analysed in the context of the information environment where information-related processes that affect the human mind occur (Ref. [80], p.3). The information environment is a complex and multi-layered concept because it consists of ICT, social and mass media and other communication channels, and the human mind perceiving, sharing, and creating ideas. NATO approach to information environment embraces all these aspects by defining it as "an environment comprised of the information itself, the individuals, organisations, and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs" [64]. Joint Publication 3-13 (JP 3-13) on Information Operations of the Joint Chiefs of Staff of the U.S. Department of Defense define the information environment as "the aggregate of individuals, organisations, and systems that collect, process, disseminate, or act on information" (Ref. [85], p. ix-x). Both definitions imply that the information environment is ubiquitous because it includes any human being, organisation, or system interacting with any information. Thereby they are too broad and nonspecific to describe how opponents use information environments to gain an advantage [27].

The division of the information environment into three dimensions (Table 11-1) better explains its complex nature and different levels of operation. Most information environment concepts divide it into three generic dimensions:

- The tangible manifestation at a physical level;
- Information itself being expressed as data, data flow, and data processing tools; and
- The human mind creating, transmitting, receiving, processing, and being affected by the information.

JP 3-13 describes the physical dimension as a tangible, real-world manifestation of information dimension, the informational dimension as data-centric, and the cognitive dimension as human-centric (Ref. [1], p. I-2). The NATO definition of *information environment* names cognitive, virtual, and physical spaces where interaction between information and individuals, organisations, and systems occurs but does not specify the spaces [64]. Ducheine et al. [25] name the dimensions of the information environment in line with terms as used in NATO definition and describe them by defining layers constituting each dimension. The UK Joint Doctrine Publication 04 (JDP 04) on Understanding (Ref. [90], p. 2-5) also divides information domain in three elements – physical for physical activity, virtual for intangible activity and cognitive for human decision-making. Cronin and Crawford (Ref. [22], p. 258) distinguish three types of assets – physical, soft, and psychic, which are targets of information warfare. Conceptually these types of assets correspond to the three dimensions of the information environment.

Table 11-1: Dimensions of the Information Environment.

JP 3-13	NATO	Ducheine et al., 2017	JDP 04	Cronin and Crawford, 1999
Physical Command and control systems, key decision makers, and supporting infrastructure	**Physical**	**Physical** Geographical, physical, and physical network layers	**Physical** Real world, facts	**Physical** Hardware, physical components of ICT
Informational Information collection, processing, storage, dissemination, protection	**Virtual**	**Virtual** Logic and virtual persona layers	**Virtual** Electronic representation	**Soft** Information and software
Cognitive The minds of those who transmit, receive, and respond to or act on information	**Cognitive**	**Cognitive** Cognitive and social layers	**Cognitive** Thought and perception	**Psychic** Perceptions, opinions, epistemology

Cyberspace is a particular and an essential part of the information environment in the digital era; however, there is no single generally accepted definition of it. The National Institute of Standards and Technology of the U.S. Department of Commerce [60] provides several definitions of cyberspace, emphasising technological aspects. One defines it as "the interdependent network of information technology infrastructures that [another definition says "and" instead of "that"] includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." Another definition complements this by adding that cyberspace is "a global domain of the information environment" [60]. The fourth definition includes the human aspect by stating that cyberspace is "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form" [60]. The Tallinn Manual 2.0, which is the research initiative of the NATO Cooperative Cyber Defence Centre of Excellence (Ref. [77], p. 564) also define cyberspace primarily in technological terms as "the environment formed by physical and non-physical components, characterised by the use of computers and the electro-magnetic spectrum to store, modify, and exchange data using computer networks." However, Ottis and Lorents [69] pointed out the insufficiencies of existing definitions and provided their definition that embraces time factor and human aspects: "cyberspace is a time-dependent set of interconnected information systems and the human".

The enormous role of computer technologies in the contemporary information environment determines that cyberspace is its essential subdomain. For example, Arquilla and Ronfeldt (Ref. [7], pp. 9-15) distinguish between cyberspace, infosphere, and noosphere as dimensions of the information environment. In their classification, cyberspace "refers to the global system of systems of internetted computers, communications infrastructures, online conferencing entities, databases, and information utilities generally known as the Net" (Ref. [7], p. 10). The infosphere includes cyberspace, media in the civilian sphere, and the electronic systems of military information environment such as "command, control, communications, intelligence, surveillance,

and reconnaissance systems" (Ref. [7], pp. 11-12). The noosphere is being defined by refereeing to the denotations of the concept proposed by Pierre Teilhard de Chardin – "globespanning realm of 'the mind,' a 'thinking circuit,' a 'stupendous thinking machine,' a 'thinking envelope' full of fibres and networks, and a planetary 'consciousness'" (Ref. [93], pp. 12-13). The noosphere is related to making sense of the information, which is the essence of the cognitive dimension.

The concept of the information environment proposed by Arquilla and Ronfeldt [7] places cyberspace at a physical dimension if compared with other concepts (Table 11-1). However, Ventre [93] proposes a different view on cyberspace because he distinguishes three layers of cyberspace that correspond to the principle of dividing the information environment into three dimensions: physical; informational, virtual or soft; and cognitive. According to the scheme developed by Ventre [93] cyberspace consists of hardware dimension, which may be attacked at a physical level; application dimension, which may be hacked; and cognitive dimension, which may be exploited by manipulating content. Thus, cyberspace is a specific domain of the information environment, but it includes the same dimensions. A similar idea is implied in the conceptualisation of "relation between environments, dimensions and domains" as developed by Ducheine et al. [25] based on the UK Development, Concepts and Doctrine Centre Joint Doctrine Publication 04 of 2010 (Ref. [25], p. 2-5), JP 3-13 (Ref. [1], pp. ix-x), and NATO Allied Joint Doctrine for Information Operations of 2015 [62].

Thus, cognitive dimension is one of the three essential parts of the information environment and cyberspace as its critical subdomain. JP 3-13 states that the cognitive dimension is "the most important component of the information environment" because in-depth understanding of the human mind is an essential precondition for influence operations, which is determined by such intangible but powerful phenomena as "individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies" (Ref. [1], p. I-3). The U.S. Department of Defense admits that cognitive dimension is "the central object of operations in the information environment" because activities at physical and informational dimensions affect the human mind (Ref. [88], p. 3). The MAGTF Information Environment Operations Concept of Employment states that information and influence operations aim to achieve "cognitive effects and psychological advantage" (Ref. [89], p. 22). At the same time, Ducheine et al. [25] conceptualise that a target actor is being affected via cognitive dimension. In a way, it is a reverse view on the role of the cognitive dimension; nevertheless, there is no contradiction because information activities affect the human mind, which determines the target's behaviour at physical environment (Figure 11-1).

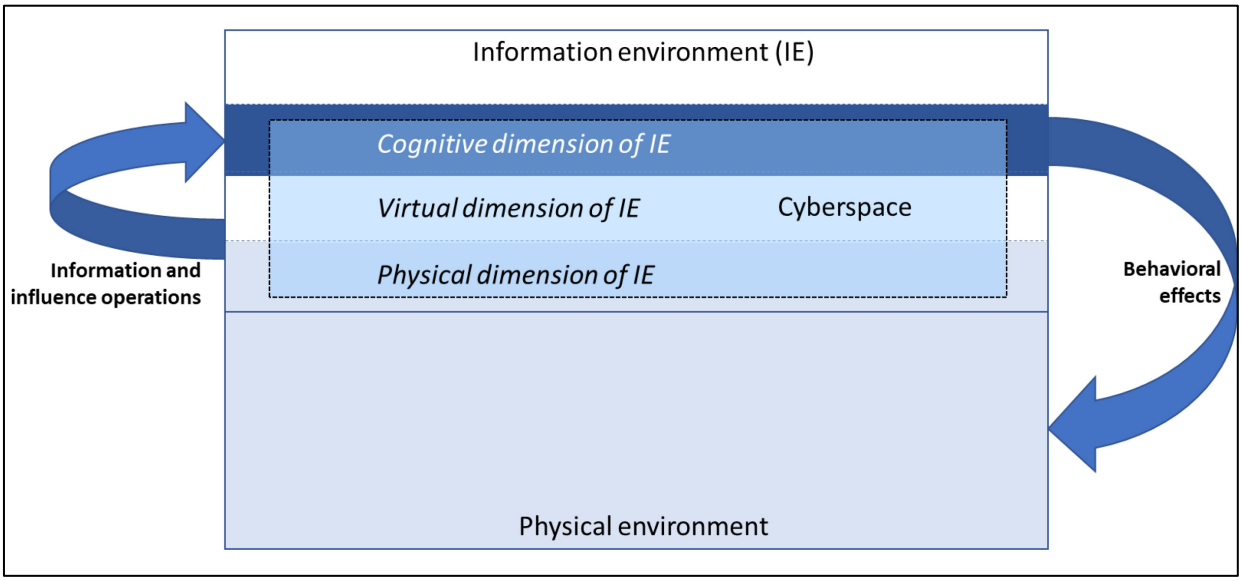

Figure 11-1: The Use of Cognitive Dimension to Achieve Political and Military Goals.

The enormous role of the cognitive dimension is determined by the fact that within it, the preconditions for behaviour form. Lippmann [49] described this process with the concept of "pseudo-environment," which is the "interior representation of the world," located between "man and his environment," and the behaviour of a man is a response to this pseudo-environment. Targeted information and influence operations at a physical and virtual dimension of the information environment, including cyberspace, affect cognitive dimension, which results in behavioural effects at the physical environment. Objects and events in the physical environment also impact the cognitive dimension. Nevertheless, as Lipmann's "pseudo-environment" concept explains, the perception of the physical environment forms through filters set up at the information environment in its broadest sense – culture, traditions, norms, history, education, and other intangible phenomena of the human mind. Thus, a human perceives the tangible world indirectly.

This peculiarity of the human mind relates cognitive aspects of social life to warfare because Clausewitz's [20] definition of war as "an act of force to compel our enemy to do our will" may be paraphrased by substituting "an act of force" with "an act of information activity." This way, operations aimed at the cognitive dimension stand out as a powerful non-kinetic tool because they allow achieving the desired effects without physical force. Nevertheless, the cognitive dimension may be affected by friendly and malign intentions. In the context of comprehensive national defence, the primary target is the cognitive dimension of domestic audiences, which requires two types of activities: the promotion of competencies, attitude, and behaviour necessary to enhance resilience and provide resistance to military and non-military aggression, and the protection from malign influence activities. Both activities relate to the issues of public opinion formation in the context of national security.

11.3 PUBLIC OPINION AS A DOMAIN OF WARFARE

Public opinion is a widely used concept; however, there is no single generally accepted definition of its essence. Manning and Romerstein (Ref. [53], p. 232) mention more than 50 definitions of public opinion. Herbst [33] classifies definitions of public opinion in four categories:

1) **Aggregation –** public opinion is a sum of individual opinions, which can be measured with sociological research methods;
2) **Majoritarian –** public opinion is a majority opinion;
3) **Discursive/Consensual –** public opinion is a result of a public discussion; and
4) **Reification –** public opinion is a fiction and a projection of elites.

Bernays's (Ref. [12], p. 61) definition illustrates the aggregation approach to the concept: "Public opinion is the aggregate result of individual opinions – now uniform, now conflicting – of the men and women who make up society or any group of society". Lawrence Lowell's idea of public opinion is majoritarian as he concludes that public opinion "must be such that while the minority may not share it, they feel bound, by conviction, not by fear, to accept it" ([46], p. 15). Luhmann [50] explains public opinion in a discursive manner as arising from "the result of the long-term effects of mass media" and describes it as "the medium of self-and world description of the modern world. It is the "Holy Spirit" of the system, the communicative availability of the results of communication". Lippmann's (Ref. [48], p.55), take on public opinion characterises it as reification: "But these manifestations [of public opinion] are in themselves nothing. They count only if they influence the course of affairs. They influence it, however, only if they influence an actor in the affair".

For the research aim of the chapter, the working definition is formulated: *public opinion is a process within the cognitive dimension of the information environment manifesting as competencies, views, and attitudes of all segments of society concerning issues of public interest*. The proposed definition emphasises several essential aspects of public opinion. First, it is a dynamic process, and an integral part of the information environment

since public opinion is simultaneously a result and an impact factor of various information flows. Second, it may be identified with sociological research methods as competencies, views, and attitudes of a society at a given time. Third, it is diverse, as different segments of society may hold different opinions. Fourth, it is related to public matters, such as governance and politics, including national security and defence.

Figure 11-2 conceptualises public opinion as a lever of power in national security and defence. The government and armed forces work out national security and defence policies, strategies, and plans. The term "government" here is used in the broadest sense as "the institutions, rules, and administration of state authority" [57]. Armed forces are subordinate to the government according to civilian control of the military [35], [38] In a democratic political system, the parliament elected by the people forms the executive branch of the government. In this sense government is subordinated to the people; therefore, the government looking for the prospects to be re-elected should be sensitive to public opinion. This way public opinion is one of the factors considered in decision-making concerning national security and defence. At the same time, communication campaigns or information and influence operations deliberately shape public opinion. Nevertheless, these campaigns and operations are not always successful because other factors also influence public opinions, such as malign foreign influence, communication campaigns of the competing political parties and interest groups, direct population experience, which contradicts messages of the government and armed forces. All this interaction takes place within the information environment as described above Figure 11-1, Figure 11-2).

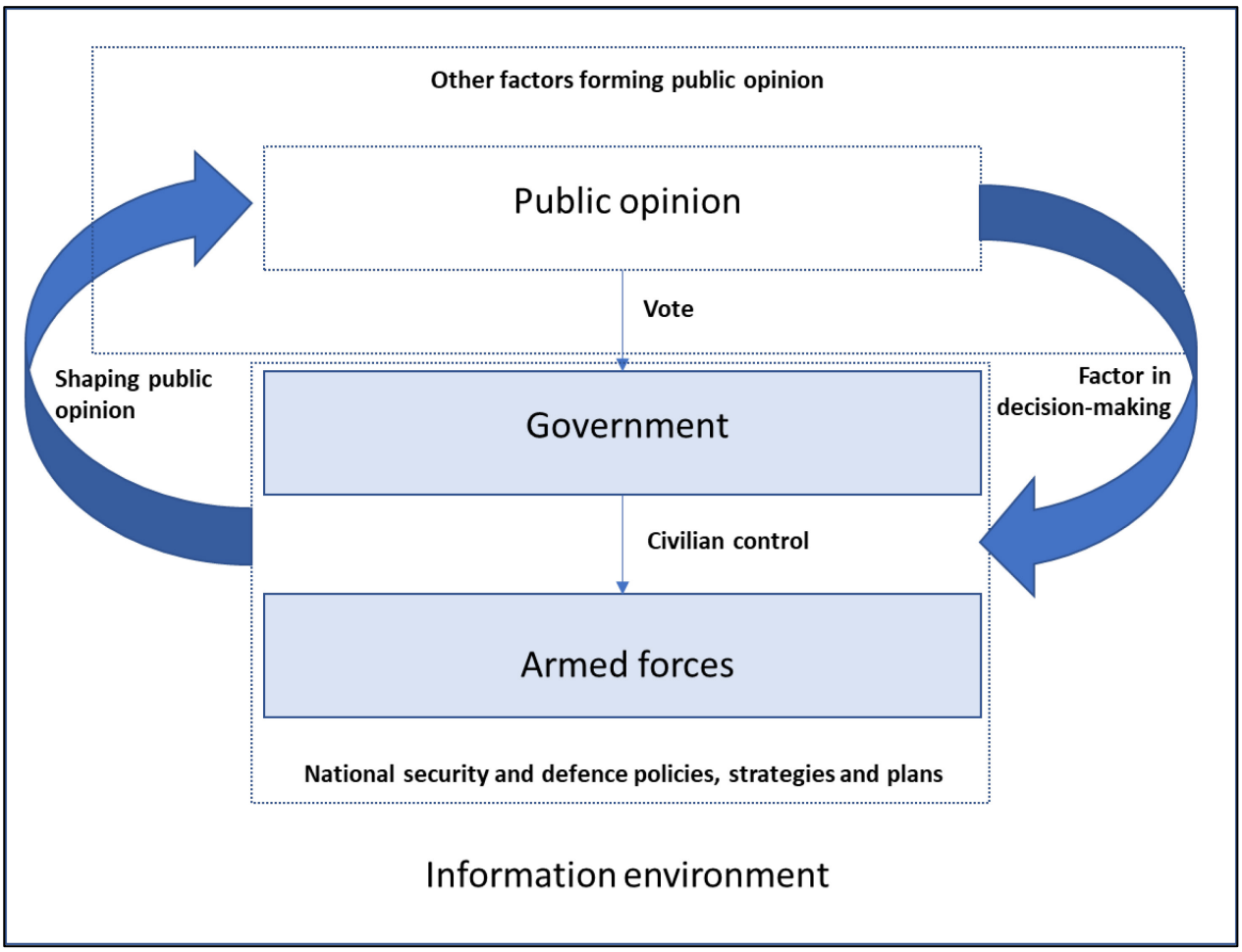

Figure 11-2: The Role of Public Opinion in National Security and Defence.

Public opinion is a factor in decision-making concerning national security and defence not only in democracies but also in authoritarian regimes. For example, Colonel general Leonid Ivashov, the Chairman of the All-Russian Officers' Assembly, in the interview to radio "Echo Moskvy" before Russia started a war against Ukraine [26] said that society is one of the forces that may prevent hostilities amid the escalation of tensions between Russia and the West from December 2021 till February 2022. In the appeal of the All-Russian Officers' Assembly to the President and citizens of the Russian Federation Ivashov named Russia's internal factors concerning elite and society relations as the cause for the escalation [36]. Russia's president Vladimir Putin also emphasised the role of public opinion when he commented an appeal of the State Duma with a request to recognise the independence of the self-proclaimed Donetsk and Lugansk People's Republics [81]: "[..] the deputies of parliament, as in any country, in Russia are guided by public opinion, by the opinion of their voters, they feel it subtly" [44]. In this case, Putin's reference to public opinion may be interpreted as a manipulation to justify Russian aggression against Ukraine; nevertheless, the quoted sentence indicates the essential role of public opinion in politics as he uses it as an excuse for the violation of the territorial integrity of Ukraine. The inherent element of Russia's military thinking is active and purposeful targeting of the cognitive domain of domestic and overseas audiences in conjunction with other instruments of power to achieve political and military goals [83].

Public opinion or media warfare is also one of the elements in the Chinese "Three Warfares" concept, which was endorsed by the Chinese Communist Party Central Committee and the Central Military Commission in 2003 (Ref. [67], p. 77). The other "two warfares" are legal and psychological, which are "force enablers in the run up to and during hostilities" being used "to undermine the spirit and ideological commitment of the adversary" (Ref. [65], p. 26). Psychological warfare targets enemy's morale and behaviour; media (or public opinion) warfare aims to influence domestic and public opinion; and legal warfare exploits international and domestic law [65]. Cheng [19] writes that psychological warfare is "the most far-reaching of the 'three warfares.' It involves the application of specialised information and media in accordance with a strategic goal and in support of political and military objectives". Lee (Ref. [47], p. 203) also notes that psychological warfare embraces other two warfares, "because public opinion warfare and legal warfare aim to achieve particular political and military goals by stimulating the psychology of one's own side or the enemy's side, which is similar to psychological warfare". Psychological warfare aims to "present one's own side as just; emphasise one's advantages; undermine the opposition's will to resist; encourage dissension in the enemy camp; implement psychological defenses" [19]. Thus, targeting public opinion is an element in military thinking for both democracies and authoritarian powers.

Nevertheless, despite the prominent role public opinion plays in politics and warfare, Boylan in 2015 wrote an article titled "Public Opinion: A Center of Gravity Leaders Forget" [16]. In Boylan's view [16], "acknowledging the necessity for developing and distributing information aimed at influencing various audiences as a decisive component of warfare" is insufficient in military thinking. Boylan [16] concludes that regardless of the increasing understanding of the role of information-related processes within the military, public opinion is still not recognised as a centre of gravity, which "risks failure to win wars". Public opinion is the end state of information activities, but it is not a sufficiently developed concept in military policies, strategies, and doctrines. For example, NATO Military Public Affairs Policy mentions "public opinion" only once, without clarifying the concept [61]. At the same time, there is a growing understanding of the role of information in warfighting. Still, the emphasis is on using information, not so much on the effects, which manifest as public opinion. It is evident in Reese's statement regarding operations in the information environment: "[..] information means increase the number of opportunities and avenues of approach to confront an adversary and can contribute as a primary defeat mechanism equivalent to, and complementary with, other physical systems" [72]. Nevertheless, how information affects the human mind and results in behaviour remains to be clarified. It is a complex process; therefore, cognitive aspects should be a distinct area of information-related domains of warfare.

The concept of cognitive warfare addresses the shortage because it emphasises the human brain as a central element of the activities in the information environment as the real target is the human mind (Ref. [24],

p. 36) Due to the increasingly decisive impact of information, Lt. Gen. Vincent R. Stewart [23], in 2017, concluded that "Fifth Generation Warfare will be Cognitive Warfare. In the twenty-first century, war is about winning the information, the decision space either before or during the conflict". Schmidt [76] states that cognitive dimension is a missing domain of warfare, nevertheless "to achieve national security objectives, protect national security interests, and prevail in modern war requires achieving cognitive superiority". The cognitive dimension of warfare includes aspects related to ICT and the human mind. Tammen [82] defines cognitive superiority as one of the five Warfare Development Imperatives in terms of the cognitive advantage of political and military leadership arising from ICT: "Truly understanding the operating environment, the adversary and the Alliance's goals entails cohesive and shared political-military understanding of the threats, adversaries and environment NATO operates in, from tech and doctrine, to JISR [Joint Intelligence, Surveillance and Reconnaissance] and big data. Equally, it will focus on providing the right tools for the political-military level to operate effectively (rapidly and dynamically) and safeguard decision-making in the modern information age". Schmidt [76] proposes to achieve cognitive superiority through "technological advantage and augmentation; education; organizational learning and adaptation; and strong leadership". Thus, technological, and soft aspects of ICT are equally important in how they affect cognitive dimension of warfighting.

The First Gulf War was a turning point in how the information age changed warfare technologically and cognitively. Berkowitz [11] writes that it was the tipping point when information technology defined military power because the U.S. and its coalition partners experienced minor damage compared to Iraq since "the Americans could see at night, drive through the featureless desert without getting lost, and put a single smart bomb on a target with a 90 percent probability." Operation Desert Storm was also an exceptional case of influencing public opinion, as formulated by Hiebert (Ref. [34], p. 243): "To win the minds at home in the recent war, the American government launched a public relations campaign on an unprecedented scale, and with unprecedented success". The First Gulf War as a media event stood out with a broad and instant media coverage, clearly defined security guidelines for journalists, a limited number of journalists having access to forbidden zones, reporters accompanied by escort officers, well-educated military leaders on public relations matters, implementation of all fundamental crisis communication principles, wide use of sound bites and visual materials, messages targeted to citizens, soldiers and adversary, the use of similar public relations principles by the opponent, managing a war like a political campaign ((Ref. [34], p. 243). In the context of the 2003 war in Iraq, Hiebert concluded that his 1991 prediction "that the battle for public opinion would be as important as the engagement of soldiers on the front" proved to be true (Ref. [34], p. 243).

This chapter focuses on public opinion; therefore, it emphasises the aspects of cognitive warfare related to public perception as an element of the contemporary battlefield. Siman-Tov and Sternberg (Ref. [79], p. 66) commenting a book written by British general Rupert Smith concluded "that in the modern world, in which communications, public opinion, and global considerations are of growing importance, concepts such as "decisive victory" are obscure and dependent upon how relevant audiences – who are not necessarily a direct part of the military campaign - perceive and recognize them". Alderman [2] claims that the mind should be defined as a distinct domain of warfare because the contemporary information environment opens up the possibility for "an amplified version of psychological warfare with the goals of dividing an enemy nation's people and leadership along social, economic, and political lines, destroying them from the inside without firing a shot". The term "the mind domain of warfare" is interchangeable with "the cognitive domain" as they describe the impact on the thought process.

Ottewell [68] defines a cognitive domain as "a domain consisting of perception and reasoning in which manoeuvre is achieved by exploiting the information environment to influence interconnected beliefs, values, and culture of individuals, groups, and/or populations," and cognitive warfare as "manoeuvres in the cognitive domain to establish a predetermined perception among a target audience in order to gain advantage over another party". Du Cluzel (Ref. [24], p. 6) defines cognitive warfare as "the way of using knowledge for a conflicting purpose". Cognitive warfare is used to attack the opponent or enemy. Rosner and Siman-Tov [74] write about "cognitive subversion" or "intervention in the 'consciousness' of another country" which is

"manipulation of the public discourse by external elements seeking to undermine social unity or damage public trust in the political system". Orinx and Struye de Swielande [66] conclude that "Western societies have become easy targets of cognitive warfare waged by adversaries like China and Russia." due to their open societies. Therefore, one of the comprehensive national defence's tasks is to counter cognitive warfare and to shape the cognitive dimension of domestic audiences to provide resistance and resilience.

11.4 THE COGNITIVE ELEMENTS OF RESISTANCE AND RESILIENCE

Resistance and resilience are the essence of comprehensive national defence. This security concept emerged during the Cold War as a defence strategy and an instrument of deterrence of non-aligned states against potential adversaries with military superiority [14]. The key idea of the concept was that a whole population mobilises against an adversary, thus raising the costs of an attack. This approach is in line with Clausewitz's idea of the resistance as the negative aim of warfare which needs "to balance any superiority the opponent may possess: in the end his political object will not seem worth the effort it costs. [..] It is evident that this method, wearing down the enemy, applies to the great number of cases where the weak endeavour to resist the strong" [20]. Therefore, implementing comprehensive national defence implies that a state will counteract military conflict and not reconcile with occupation.

Clausewitz defines resistance as "a form of action, aimed at destroying enough of the enemy's power to force him to renounce his intentions" [20]. Anderson (Ref. [6], pp. 37-38) studied historical cases of small states resisting great power aggression, and concluded that "mere technical supremacy is not enough" because there are other preconditions for the effective occupation such as collaboration of the occupied population; the absence of ethnic and religious motives to resist; limited casualties in the civilian population; restoration of economics; protection of civil population from insurgents; political support from the domestic audiences and elites; and financial resources. Martin (Ref. [55], p. 4) distinguishes "national resistance" and "community resistance," which is relevant in the context of comprehensive national defence as both types are essential for successful resistance. By "national resistance," he means military defence, but "community resistance" is "nonviolent community resistance to aggression as an alternative to military defence" (Ref. [55], p. 4). Both military and nonviolent resistance methods are essential to resist aggressors with military superiority.

Resistance is closely related to the concept of resilience. Fiala (Ref. [29], p. 5) describes this as "a synergistic relationship [that] exists between ongoing government planning and preparation activities that foster national resilience and defend sovereignty, and how these activities contribute to resistance conducted to regain national sovereignty". The European Commission (Ref. [28], p. 6) defines resilience as "the ability not only to withstand and cope with challenges but also to transform in a sustainable, fair, and democratic manner". This definition is based on Manca, Benczur, and Giovannini (Ref. [52], p. 5) approach to three capacities of a resilient society: the absorptive capacity to resist "shocks or persistent structural changes"; the adaptive capacity to make minor flexible changes; and the transformative capacity to change the system. NATO defines resilience as "a society's ability to resist and recover from such shocks and combines both civil preparedness and military capacity" [63]. The first two days of Russia's invasion in Ukraine, on February 24, 2022, demonstrated how this theory works in practice as Ukrainian leaders, armed forces, and society demonstrated an outstanding military resistance and psychological resilience and caused substantial damage to the aggressor with significant military superiority.

The readiness to defend a country requires prerequisites and preparedness at the physical and cognitive levels. Sufficient military equipment, the acquisition of basic military skills and involvement in national defence by a considerable part of the population, pre-planning and preparation for resistance operations, and previously established organisational structures are some of the fundamental elements. At the same time, the resistance operations due to their predominantly decentralised nature, especially if the civilian population is being involved, may happen if society has a will to defend their country. The cognitive dimension primarily

determines this aspect of resistance and resilience, and it will be further elaborated in detail. Academic studies have identified several factors that positively affect willingness to defend a country. Rutkauskas [75] and Torgler [87] discovered such factors as national pride, confidence in government, and confidence in the armed forces. In addition to these, Berzina and Zupa [15] identified factors such as crisis preparedness, threat perception, historical heroism, and media consumption. Fiala (Ref. [29], pp. 7-11) names prerequisites for resistance such as national identity; psychological preparation; knowledge of vulnerabilities; vulnerability reduction; potential external threat identification; preparation against the threat – international, interoperability with external supporters, and domestic. Figure 11-3 structures and lists the proposed elements of the cognitive dimension according to the functions of the human mind – accumulation of competencies including necessary knowledge and skills, formulation of opinion, and generation of affect. It is based on previous findings and adds additional elements by answering the question of what competencies, views, and attitudes are necessary to provide resistance and resilience?

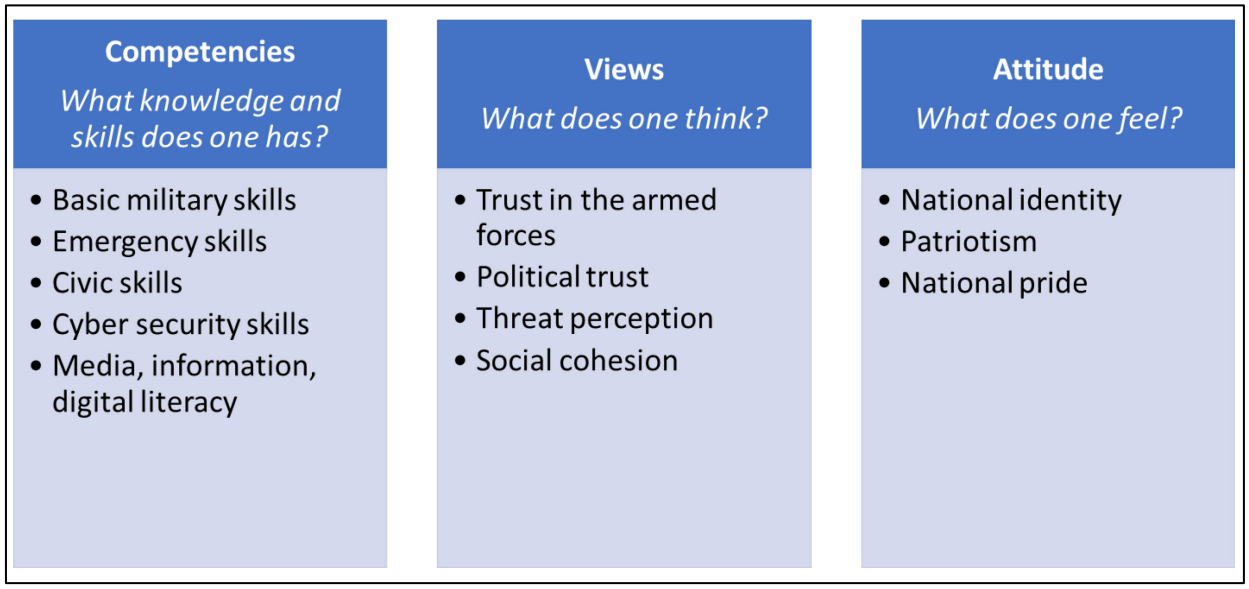

Figure 11-3: Elements of the Cognitive Dimension of Comprehensive National Defence.

11.4.1 Competencies

To resist aggression effectively, a large part of society needs to be militarily trained because the readiness of soldiers for military operations is one of the factors determining the success of the army. Thus, one of the key questions for the effective comprehensive national defence is how to ensure that as many people as possible have acquired basic military skills? Compulsory military service is the most obvious instrument historically and nowadays for "turning civilians into soldiers" (Ref. [56], p. 37). However, there was the decline of conscription in the West after the Second World War (Ref. [37], pp. 57-59) and the transition to all-volunteer forces in NATO member states after the Cold War [94]. There is an ongoing debate if the compulsory military service is the most effective way to build reserve forces. For example, Poutvaara and Wagener [71], argue that conscription does not provide better reserves "if reservists are not appropriately prepared for their assignments in case of mobilization." There are also economic, social, and political factors determining if there is a support for compulsory military service in a country [8]. The acquisition of basic military skills must consider the peculiarities of modern warfare, the need for regular updating of military skills [17], [32], as well as the values of society and its economic, social and political structures [10], [54]. Thus, there may be different forms of the basic military training of society, for example, Latvia will introduce mandatory military training at secondary schools from 2024 [92].

Emergency preparedness skills at the individual level also is a prerequisite for resilience since knowing the right type of behaviour in various types of disaster may significantly reduce casualties and losses. The skills can be acquired through the education and training, which is an essential part of civil protection system. Alexander (Ref. [3], p. 272) distinguishes several elements of the civil protection education and training: a culture of professionalism in the civil protection field; cooperation with academic institutions; a national emergency training program; consensus on the emergency training curriculum; participation in professional associations; professional standards of emergency managers. All these efforts contribute to the so-called "culture of preparedness" [39], [70], [40], which implies the necessary preconditions at the cognitive dimension to deal with disasters at the individual, local, regional, and national levels.

Whole-of-society involvement in national defence requires the capability of "working collectively to achieve common interests" (Ref. [41], p. 572), which is one of the integral elements of civic skills. The comprehensive national defence system, to a large extent, requires voluntary participation and contribution to national defence, therefore it may be assumed that the development of "foundational civic skills such as working in groups, organizing others to accomplish tasks, communicating, and working out differences of substance or process on the way to accomplishing a goal" (Ref. [41], p. 573) may be crucial for societal resilience during the military conflict. A long-term developed civil society network may provide invaluable assistance to government and force structures in overcoming any crisis, including military conflicts. The development of civic skills takes place through civic education in schools, universities, and life-long learning programs. Civic education is crucial in yet another aspect – to provide for the sustainability of democracy through civic engagement and participation, as democratic values are one of the NATO foundational principles. Strengthening democratic values is essential considering the increasing role of authoritarian power centres like China.

Due to the enormous role information and communication technologies plays in contemporary society, the spread of disinformation and cyber-attacks are characteristic features of contemporary military crises. Therefore, to diminish malign influence in the information environment, information environment-related literacies and cybersecurity skills of a significant part of society are preconditions for a resilient society. University of Iowa Center for Teaching [91] distinguishes five types of literacy: media literacy – the ability to think critically about information obtained on any type of media; computer literacy – the ability to use computer hardware and software; digital literacy – a sum of cognitive skills necessary to operate in digital environment; information literacy – the ability to use information; technology literacy – the ability to use information and communication technologies.

Cybersecurity is a vast area requiring policies and actions at international, national, local, and individual levels. However, within the cognitive dimension of comprehensive national defence, cybersecurity skills at the individual level are of primary importance. This way, the whole-of-society resilience towards cyberattacks is increased. Carlton and Levy [18] name several essential cybersecurity skills for non-IT specialists:

> *...preventing the leaking of confidential digital information to unauthorized individuals; preventing malware via non-secure Websites; preventing personally identifiable information (PII) theft via access to non-secure networks; preventing PII theft via e-mail phishing; preventing malware via e-mail; preventing credit card information theft by purchasing from non-secured Websites; preventing information system compromise via USB or storage drive/device exploitations; preventing unauthorized information system access via password exploitations; preventing PII theft via social networks.*

All these skills may be obtained and developed by increasing the knowledge about the described areas and applying it to the practice.

11.4.2 Views

The effectiveness of comprehensive national defence also depends on society's social and political views. First, the population should trust its armed forces because they provide military resistance to aggressors. The belief in the capacity of the armed forces to defend a country is crucial for the rest of society to involve in national or community resistance because people need faith in victory. Trust in the armed forces results from complex and context-specific circumstances, such as political regimes, involvement in military conflicts, economic development, and others [58], [86]. Overall, armed forces are among the most trusted institutions globally [31]; nevertheless, it is an indicator to be monitored and sustained through effective civil-military relations.

Second, political leaders lead the resistance movement; therefore, political trust is essential. Trust in political leaders results from a long-term effort to build strong state and society relations. Nevertheless, the theory has identified the so-called "the rally round the flag" effect, which describes the phenomenon that in times of crisis, people tend to support their political leaders (Ref. [59], p. 21). This effect was visible after Russia invaded Ukraine in 2022 when the approval rating of Ukraine's president Volodymir Zelensky increased from 31 % in December 2021 to 91 % in February 2022 [30]. However, a society can be more resilient if it has trustful state-society relations even before the crisis. Political trust in democracies is determined by political and economic performance, limited corruption, governmental responsiveness, leadership, partisanship, freedoms, and other factors (Ref. [13], p. 3).

Third, the perception of the threats also determines involvement in national defence because an opponent or adversary may attempt to deceive about its peaceful intention, which decreases the alertness of a society under attack. Educating the public about the strategy and tactics of the enemy is essential for having a realistic assessment of the security situation. Latvia is an example of the polarisation of views in relation to threat perception according to a 2019 survey data. 60 % of respondents using the Latvian language at home considered Russia's policy to be a threat to Latvia's, whereas only 15 % of Russian speakers agreed with it (Ref. [15], p. 26). The view that a country has no military threats decreases the willingness to fight for a country.

The polarisation of views also indicates an issue of social cleavage. It is an obstacle to the whole-of-society approach because an effective response to disasters, including military attacks, requires a unified response from a significant part of the population. Thus, social cohesion is an essential building block of comprehensive national defence. The Department of Economic and Social Affairs of the United Nations Secretariat [84] provides a working definition of the concept: "[..] A socially cohesive society is one where all groups have a sense of belonging, participation, inclusion, recognition and legitimacy. Such societies are not necessarily demographically homogenous. Rather, by respecting diversity, they harness the potential residing in their societal diversity (in terms of ideas, opinions, skills, etc.). Therefore, they are less prone to slip into destructive patterns of tension and conflict when different interests collide". The Social Cohesion Framework (Ref. [78], p. 12) distinguishes three building blocks within the theoretical concept of social cohesion: "social relationships (social networking, participation, trust); connectedness (feeling of belonging, identification); and orientation towards the common good (social responsibility, solidarity, recognition of the social order and rules)". Achieving social cohesion in a divided society requires long-term national, regional and local policies to implement unified fundamental democratic values, which consolidate society for a common goal in crises.

11.4.3 Attitude

The emotional aspect also is essential as it is a powerful determinant of human behaviour. In the will to defend a country, national identity is substantial because it determines the purpose of resistance. Renan (Ref. [73], p. 52) calls the nation "a soul, a spiritual principle." Connor (Ref. [21], p. 92) notes that the intangible aspect of a nation is what makes it challenging to define the concept because its essence is

"a psychological bond that joins a people and differentiates it, in the subconscious conviction of its members, from all other people in a most vital way." Likewise, Anderson's (Ref. [5], p. 6) definition of a nation as an "imagined political community" emphasises the intangible aspect. Thus, national identity manifests itself in the cognitive realm as emotions and ideas related to a membership in a social group. As formulated by Kohn [42]: "Nationalism is an idea, an idée-force, which fills man's brain and heart with new thoughts and new sentiments, and drives him to translate his consciousness into deeds of organized action". In military conflicts, an adversary aims to attack also the national identity of a target, which was evident in the pre-war speech by V. Putin [43] during Russia's military aggression against Ukraine in February 2022. On the other hand, a solid national identity gives an idea and inspiration for society to defend its core values and the meaning of existence.

This sentiment is closely related to national pride and patriotism. Patriotism is an emotional attachment to one's country that implies readiness to die for the country when under attack. In simple terms, patriotism means "a love for one's country" however, a theory has a variety of definitions of the concept and a broad debate regarding its moral substance and issues. According to Audi (Ref. [9], p. 367) "[t]he term "patriotism" may be used to designate at least three different kinds of things: a trait of character, as where we speak of a person who is patriotic to the core; an emotion, as where people are described as glowing with patriotism or bursting with pride in their country; and (perhaps by extension from these more basic cases) a position, such as the view that one owes loyalty to one's country." MacIntyre (Ref. [51], p. 4) defines patriotism" in terms of a kind of loyalty to a particular nation which only those possessing that particular nationality can exhibit.[..] Patriotism is not to be confused with a mindless loyalty to one's own particular nation which has no regard at all for the characteristics of that particular nation. Patriotism does generally and characteristically involve a peculiar regard not just for one's own nation, but for the particular characteristics and merits and achievements of one's own nation."

All these aspects may and should be cultivated and promoted in a society in the long term. For democratic societies it is crucial to develop civic type of patriotism to sustain democratic values. As stressed by Laborde (Ref. [45], p. 599):

> *[c]ivic patriots have always subordinated their allegiance to a country to their love of liberty, even if it is their allegiance to this or that particular polity which coloured their understanding of liberty. In other words, a patriot should not say 'my country right or wrong', but rather 'my country for the values it represents (or should represent)'.*

11.5 CONCLUSIONS AND RECOMMENDATIONS

This chapter has explained the cognitive dimension as one of the three dimensions of the information environment and cyberspace as its subdomain. The cognitive dimension is related to the human mind, which is an essential domain of warfare in the information age in the view of prominent military experts. By manipulating the cognitive dimension with information and influence operations it is possible to achieve behavioural effects without using physical force. The processes in the cognitive dimension at a societal level manifest as public opinion, which is one of the levers of power in national security as it is a factor in the decision-making process. The prominent role of public opinion is determined by democratic civil-military control; nevertheless, authoritarian regimes also exploit public opinion to achieve their political and military goals. For the comprehensive national defence to be effective, the willingness to defend and fight for a country is an essential precondition at the cognitive dimension. It results from the long-term trends and various elements in terms of knowledge, views, and attitudes concerning national defence and state and society relations.

To develop and sustain resilience and resistance at a cognitive dimension within the comprehensive national defence, it is recommended:

1) To conceptualise public opinion as the end state of information activities in NATO military policies, strategies, and doctrines.
2) To ensure the mass acquisition of basic military skills in a way that is best suited to the historical, social, political, and economic specificities of a given society.
3) To ensure the mass acquisition of emergency preparedness skills at individual, organisational, self-government, and national levels.
4) To develop civic education programs in schools, higher education establishments, and lifelong learning programs, as it develops civic skills necessary for the sustainability of democracy and the capabilities to involve in national defence by the whole of society.
5) To develop education programs for young people and adults to develop information environment-related literacies and cyber security skills.
6) To monitor and sustain trust in the armed forces through effective civil-military relations.
7) To enhance political trust by increasing government responsiveness to societal needs, the efficiency of the public administration apparatus, economic welfare, and the improvement of other macro-level political, social, and economic factors.
8) To develop targeted strategic communication programs to explain security policies and their broader context for various groups of society, considering their established views, media consumption, and other specifics.
9) To develop strategies and policies of social cohesion at local, regional, and national levels.
10) To develop strategic communication programs for strengthening national identity and enhancing civic patriotism among young people and adults.

11.6 REFERENCES

[1] The Joint Chiefs of Staff (2012), Joint Publication 3-13 Information Operations, November 27, Incorporating Change 1 November 20, 2014, available https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf Accessed May 25, 2021).

[2] Alderman, R. (2017), "Domains of warfare and strategic offsets", Military Embedded Systems, January 31, available https://militaryembedded.com/comms/satellites/domains-of-warfare-and-strategic-offsets Accessed February 23, 2022.

[3] Alexander, D.E. (2015), "Evaluation of civil protection programmes, with a case study from Mexico", Disaster Prevention and Management, 24(2), 263-283, doi: 10.1108/DPM-12-2014-0268.

[4] American Psychological Association (n.d.), Cognition. APA Dictionary of Psychology, available https://dictionary.apa.org/cognition Accessed January 19, 2022.

[5] Anderson, B. (1996), Imagined Communities: Reflections on the Origin and Spread of Nationalism. Revised Edition. London: Verso.

[6] Anderson, R. D. (2005), "Lessons from history on the limits of imperialism: Successful small state resistance to great power aggression", Journal of Third World Studies, 22(1), 21-40, available https://www.jstor.org/stable/45194220 Accessed February 24, 2022.

[7] Arquilla, J. and Ronfeldt, D. (1999), The Emergence of Noopolitik: Toward an American Information Strategy. Santa Monica, CA: RAND.

[8] Asal, V., Conrad, J., and Toronto, N. (2015), "I want you! The determinants of military conscription", Journal of Conflict Resolution, 61(7), pp. 1456-1481. doi:10.1177/0022002715606217.

[9] Audi, R. (2009), "Nationalism, patriotism, and cosmopolitanism in an age of globalization", The Journal of Ethics, 13(4), pp. 365-381, available http://www.jstor.org/stable/25656267 Accessed May 28, 2022.

[10] Barno, D. and Bensahel, N. (2018), "The deepest obligation of citizenship: Looking beyond the warrior caste", War On the Rocks, May 15, available https://warontherocks.com/2018/05/the-deepest-obligation-of-citizenship-looking-beyond-the-warrior-caste/ Accessed April 27, 2022.

[11] Berkowitz, B. (2010), The New Face of War. [ebook]. New York: Free Press, available https://www.perlego.com/book/779435/the-new-face-of-war-pdf Accessed February 12, 2022.

[12] Bernays, E. [1923] (1961), Crystallizing Public Opinion. New York: Liveright Publishing Company.

[13] Berzina, I. (2018), "Political trust and Russian media in Latvia", Journal on Baltic Security,4(2), pp. 2-9. doi: 10.2478/jobs-2018-0008.

[14] Berzina, I. (2020), "From 'total' to 'comprehensive' national defence: The development of the concept in Europe", Journal on Baltic Security, 6(2), 7-15, doi: 10.2478/jobs-2020-0006.

[15] Berzina, I. and Zupa, U. (2019), Latvijas sabiedrības griba aizstāvēt valsti: veicinošie un kavējošie faktori ["The will of Latvian society to defend the state: Facilitating and disincentive factors"], National Defence Academy of Latvia, Center for Security and Strategic Studies, available https://www.naa.mil.lv/sites/naa/files/document/DSPC_GribaAizstavetValsti_0.pdf Accessed February 25, 2022.

[16] Boylan, S. (2015), Public opinion: A center of gravity leaders forget," Military Review, September-October, pp. 93-105, available https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20151031_art015.pdf Accessed February 11, 2022.

[17] Bryant, D.J. and Angel, H. (2000), "Retention and fading of military skills: Literature review", Technical Report, DCIEM No. CR 2000-070.

[18] Carlton, M. and Levy, Y. (2015), "Expert assessment of the top platform independent cybersecurity skills for non-IT professionals", SoutheastCon 2015, pp. 1-6, doi: 10.1109/SECON.2015.7132932.

[19] Cheng, D. (2013), "Winning without fighting: The Chinese psychological warfare challenge", The Heritage Foundation, July 12, available https://www.heritage.org/global-politics/report/winning-without-fighting-the-chinese-psychological-warfare-challenge Accessed February 23, 2022.

[20] Clausewitz, C.V. [1780 – 1831], On War. [ebook 2008]. Princeton: Princeton University Press, available https://www.perlego.com/book/735246/on-war-pdf Accessed February 10, 2022.

[21] Connor, W. (1994), Ethnonationalism: the Quest for Understanding. New Jersey: Princeton University Press.

[22] Cronin, B. and Crawford, H. (1999), "Information warfare: Its application in military and civilian contexts", The Information Society, 15:4, 257-263, doi: 10.1080/019722499128420.

[23] Defense Intelligence Agency (2017), "Lt. Gen. Stewart's remarks at DoDIIS17, August 15", available https://www.youtube.com/watch?v=Nm-lVjRjLD4&t=372s Accessed February 16, 2022.

[24] Du Cluzel, F. (2020), "Cognitive warfare", Innovation Hub, available https://www.innovationhub-act.org/sites/default/files/2021-01/20210113_CW%20Final%20v2%20.pdf Accessed February 23, 2022.

[25] Ducheine, P.A.L., van Haaster, J., and van Harskamp, R. (2017), "Manoeuvring and Generating Effects in the Information Environment", in P.A.L. Ducheine and F.P.B. Osinga (Eds.), Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises (pp. 155-179). NL ARMS: Netherlands Annual Review of Military Studies; Vol. 2017, Asser Press, available doi: 10.1007/978-94-6265-189-0_9 Accessed August 16, 2022.

[26] Echo Moskvy (2022), Путину надоела Россия - Отставной генерал Ивашов о войне с Украиной ["Putin tired of Russia – Retired General Ivashov about the war with Ukraine"], February 8, available https://www.youtube.com/watch?v=iXOcuzQjzdo Accessed February 16, 2022.

[27] Ehlers Jr., R.S. and Blannin, P. (2020), "Making sense of the information environment", Small Wars Journal, available https://smallwarsjournal.com/jrnl/art/making-sense-information-environment#_edn6 Accessed January 31, 2022.

[28] European Commission (2020), "Strategic foresight report – Charting the course towards a more resilient Europe", September 9, available https://ec.europa.eu/info/sites/default/files/strategic_foresight_report_2020_1_0.pdf Accessed February 25, 2022.

[29] Fiala, O.C. (2020), Resistance Operating Concept. The JSOU Press, available https://jsou.libguides.com/ld.php?content_id=54216464 Accessed February 24, 2022.

[30] Fitri, A. (2022), "How President Zelensky's approval ratings have surged", The New Statesmen, March 1, available https://www.newstatesman.com/chart-of-the-day/2022/03/how-president-zelenskys-approval-ratings-have-surged Accessed May 27, 2022.

[31] Garb, M. (2015), "Public trust in the military: The Slovenian Armed Forces in a comparative analysis", Current Sociology, 63(3), pp. 450-469. doi: 10.1177/0011392114566351.

[32] Henik, A., Brainin, E., Ze'evi, V. and Schwarz, D. (1999), "The preservation and the decay of military skills", Final report for project: R&D 7699-RB-01.

[33] Herbst, S. (1993), "The meaning of public opinion: Citizens' constructions of political reality", Media, Culture & Society, 15(3), pp. 437-454. doi:10.1177/016344393015003007.

[34] Hiebert, R.E. (2003), "Public relations and propaganda in framing the Iraq war: A preliminary review", Public Relations Review, 29, 243-255. doi: 10.1016/S0363-8111(03)00047-X.

[35] Huntington, S. (1981), The Soldier and the State: The Theory and Politics of Civil-Military Relations. Cambridge: The Belknap Press of Harvard University Press.

[36] Ivashov, L.G. (2022), Обращение Общероссийского офицерского собрания к президенту и гражданам Российской Федерации ["Appeal of the all-Russian Officers' Assembly to the President and citizens of the Russian Federation"], available http://ooc.su/news/obrashhenie_obshherossijskogo_oficerskogo_sobranija_k_prezidentu_i_grazhdanam_rossijskoj_federacii/2022-01-31-79 Accessed February 16, 2022.

[37] Janowitz, M. (1983), The Reconstruction of Patriotism: Education for Civic Consciousness. Chicago: The University of Chicago.

[38] Janowitz, M. (1988), The Professional Soldier: A Social and Political Portrait. New York: Free Press.

[39] Kapucu, N. (2008), "Culture of preparedness: Household disaster preparedness", Disaster Prevention and Management, 17(4), 526-535. doi: 10.1108/09653560810901773.

[40] Kapucu, N., and Khosa, S. (2013), "Disaster resiliency and culture of preparedness for university and college campuses", Administration & Society, 45(1), pp. 3-37. doi: 10.1177/0095399712471626.

[41] Kirlin, M. (2002), "Civic skill building: The missing component in service programs?" Political Science & Politics, 35(03), pp. 571-575. doi:10.1017/s1049096502000872.

[42] Kohn, H. [1944], The Idea of Nationalism: A Study in Its Origins and Background. [ebook 2017] 1st edn. Oxon: Routledge, available https://www.perlego.com/book/1578556/the-idea-of-nationalism-pdf Accessed May 28, 2022.

[43] Kremlin (2021), Обращение Президента Российской Федерации ["Address of the President of the Russian Federation"], February 21, available http://kremlin.ru/catalog/countries/UA/events/67828 Accessed February 25, 2022.

[44] Kremlin.ru (2022), Пресс-конференция по итогам российско-германских переговоров ["Press conference following Russian-German talks"], February 15, available http://kremlin.ru/events/president/news/67774 Accessed February 16, 2022.

[45] Laborde, C. (2002), "From constitutional to civic patriotism", British Journal of Political Science, 32(4), pp. 591-612, available http://www.jstor.org/stable/4092375 Accessed May 28, 2022.

[46] Lawrence Lowell, A. (1913), Public Opinion and Popular Government. New York: Longmans, Green, and Co.

[47] Lee, S. (2014), "China's 'three warfares': Origins, applications, and organizations", Journal of Strategic Studies, 37:2, pp. 198-221. Doi: 10.1080/01402390.2013.870071.

[48] Lippmann, W. (1930), The Phantom Public: A Sequel to "Public Opinion". New York: The Macmillan Company.

[49] Lippmann, W. [1922], Public Opinion. [ebook 2016]. Lanham: Dancing Unicorn Books, available https://www.amazon.com/Public-Opinion-Walter-Lippmann-ebook/dp/B01NBJW9S7 Accessed February 10, 2022.

[50] Luhmann, N. [1997], Theory of Society, Volume 2. 1st ed. [ebook 2013]. Stanford: Stanford University Press, available https://www.perlego.com/book/745824/theory-of-society-volume-2-pdf Accessed February 13, 2022.

[51] MacIntyre, A. (1984), "Is Patriotism a Virtue?", The Lindley Lecture, The University of Kansas.

[52] Manca, A.R., Benczur, P. and Giovannini, E. (2017), "Building a scientific narrative towards a more resilient EU society", Joint Research Centre (JRC), the European Commission's science and knowledge service, available https://publications.jrc.ec.europa.eu/repository/handle/JRC106265 Accessed February 25, 2022.

[53] Manning, M.J. and Romerstein, H. (2004), Historical Dictionary of American Propaganda. Westport: Greenwood Press.

[54] Margulies, M. (2018), "The greatest sacrifice: Why military service should not be an obligation of citizenship", War On the Rocks, May 31, available https://warontherocks.com/2018/05/the-greatest-sacrifice-why-military-service-should-not-be-an-obligation-of-citizenship/ Accessed April 27, 2022.

[55] Martin, B. (1993), Social Defence, Social Change. London: Freedom Press.

[56] Matthews, M.D. (2020), Head Strong: How Psychology is Revolutionizing War. New York: Oxford University Press.

[57] McLean, I. and McMillan, A. (2009), The Concise Oxford Dictionary of Politics (3rd ed.). Oxford: Oxford University Press.

[58] Montalvo, D. (2009), "Do you trust your Armed Forces? ", LAPOP-AmericasBarometer Insights Series Compilation, I, Insights Reports 1-30, 2008 – 2009, pp. 146-150.

[59] Mueller, J.E. (1970), "Presidential popularity from Truman to Johnson", The American Political Science Review, 64 (1), pp. 18-34.

[60] National Institute of Standards and Technology (n.d.), "Cyberspace", Computer Security Resource Center, available https://csrc.nist.gov/glossary/term/cyberspace Accessed February 1, 2022.

[61] NATO (2011), NATO Military Public Affairs Policy, MC 0457/2, February, available https://www.nato.int/ims/docu/mil-pol-pub-affairs-en.pdf Accessed February 17, 2022.

[62] NATO (2015), Allied Joint Doctrine for Information Operations, AJP-3.10 (Edition A Version 1 ed).

[63] NATO (2021), "Resilience and Article 3", June 11, available https://www.nato.int/cps/en/natohq/topics_132722.htm Accessed February 25, 2022.

[64] NATO (2021), NATO Glossary of Terms and Definitions, AAP-06 (English and French).

[65] Office of the Secretary of Defense (2011), "Military and security developments involving the People's Republic of China", Annual Report to Congress, available https://dod.defense.gov/Portals/1/Documents/pubs/2011_CMPR_Final.pdf Accessed February 23, 2022.

[66] Orinx, K. and Struye de Swielande, T. (2021), "Cognitive warfare and the vulnerabilities of democracies", CECRI, available http://cecrilouvain.be/wp-content/uploads/2021/05/cognitive-warfare-.pdf Accessed February 24, 2022.

[67] Ota, F. (2014), "Sun Tzu in contemporary Chinese strategy", Joint Force Quarterly, 2nd Quarter, pp. 76-80.

[68] Ottewell, P. (2020), "Defining the Cognitive Domain", OTH, December 7, available https://othjournal.com/2020/12/07/defining-the-cognitive-domain/ Accessed February 16, 2022.

[69] Ottis, R. and Lorents, P. (2010), "Cyberspace: Definition and implications", in Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8 – 9 April 2010. Reading: Academic Publishing Limited, pp. 267-270.

[70] Parker, C.L., Barnett, D.J., Fews, A.L., Blodgett D. and Links, J.M. (2005), "The road map to preparedness: A competency-based approach to all-hazards emergency readiness training for the public health workforce", Public Health Rep. Sep-Oct;120(5), 504-14. Doi: 10.1177/003335490512000505.

[71] Poutvaara, P. and Wagener, A. (2011), "Ending Military Conscription", CESifo DICE Report, ISSN 1613-6373, ifo Institut – Leibniz-Institut für Wirtschaftsforschung an der Universität München, München, 09(2), pp. 36-43.

[72] Reese, T. (2020), "Operations in the information environment", Marine Corps Gazette, August, WE31-WE39, p. WE31.

[73] Renan, E. [1882] (1996), "What Is a Nation?", in G. Eley and R.G. Suny (Eds.), Becoming National: A Reader. Oxford: Oxford University Press.

[74] Rosner, Y. and Siman-Tov, D. (2018), "Russian intervention in the US presidential elections: The New threat of cognitive subversion", INSS Insight 1031, March 8, available https://www.inss.org.il/publication/russian-intervention-in-the-us-presidential-elections-the-new-threat-of-cognitive-subversion/ Accessed February 24, 2022.

[75] Rutkauskas, V. (2018), "Factors affecting willingness to fight for one's own country: The case of Baltic states", Special Operations Journal, 4(1), pp. 48-62, p. 60. doi: 10.1080/23296151.2018.1456286.

[76] Schmidt, T. (2020), "The missing domain of war: Achieving cognitive overmatch on tomorrow's battlefield", Modern War Institute, July 4, available https://mwi.usma.edu/missing-domain-war-achieving-cognitive-overmatch-tomorrows-battlefield/ Accessed February 23, 2022.

[77] Schmitt, M.N. (Ed.) (2017), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd Edition). Cambridge: Cambridge University Press.

[78] Search For Common Ground (2017), "The Social Cohesion Framework: Social Cohesion for Stronger Communities", available https://www.sfcg.org/wp-content/uploads/2017/02/SC2_Framework-copy.pdf Accessed May 27, 2022.

[79] Siman-Tov, D. and Sternberg, D. (2017), "The Missing effort: Integrating the 'Non-lethal' dimension in the Israeli military lines of operation", Cyber, Intelligence, and Security, 1(3), 65-81, available https://www.inss.org.il/wp-content/uploads/2018/01/CyberENG1.3_6-67-83.pdf Accessed February 23, 2022.

[80] Slack, K. (2019), The Information Lever of Power. Freeman Air & Space Institute, available https://www.kcl.ac.uk/warstudies/assets/information-lever-of-power.pdf Accessed February 23, 2022.

[81] Svidrigailov, G. (2022), Госдума поддержала обращение к президенту России о признании ДНР и ЛНР ["The State Duma supported the appeal to the President of Russia on the recognition of the DNR and LNR"], Gazeta.ru, available https://www.gazeta.ru/politics/news/2022/02/15/17293801.shtml Accessed February 16, 2022.

[82] Tammen, J.W. (2021), NATO's warfighting capstone concept: Anticipating the changing character of war", NATO Review, July 9, available https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html Accessed February 17, 2022.

[83] Tashev, B., Purcell, M. and McLaughlin, B. (2019), "Russia's information warfare: Exploring the cognitive dimension", MCU Journal, 10(2), pp. 129-147, doi: 10.21140/mcuj.2019100208 Accessed February 23, 2022.

[84] The Department of Economic and Social Affairs of the United Nations Secretariat (n.d.), "E-Dialogue "Creating an Inclusive Society: Practical Strategies to Promote Social Integration", available https://www.un.org/esa/socdev/sib/inclusive_society/social%20cohesion.html Accessed May 27, 2022.

[85] The Joint Chiefs of Staff (2012), Joint Publication 3-13 Information Operations, November 27, Incorporating Change 1 November 20, 2014. available https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf Accessed May 25, 2021).

[86] Tiargan-Orr, R., and Eran-Jona, M. (2016), "The Israeli public's perception of the IDF: Stability and change", Armed Forces & Society, 42(2), pp. 324-343. doi: 10.1177/0095327X15592214.

[87] Torgler, B. (2003), "Why do people go to war?", Defence and Peace Economics, 14(4), pp. 261-280. doi: 10.1080/10242690302929.

[88] U.S. Department of Defense (2016), "Strategy for operations in the information environment", available https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf Accessed February 5, 2022.

[89] U.S. Marine Air Ground Task Force (2017), "Information environment operations concept of employment", available https://www.trngcmd.marines.mil/Portals/207/Docs/wtbn/MCCMOS/FINAL%20MAGTF%20IE%20OPS%20CoE%202017-07-06.pdf?ver=2017-11-16-090225-057 Accessed February 6, 2022.

[90] UK Development, Concepts and Doctrine Centre (2010), Joint Doctrine Publication 04: Understanding, December.

[91] University of Iowa Center for Teaching (n.d.), "Types of literacies", available https://teach.its.uiowa.edu/sites/teach.its.uiowa.edu/files/docs/docs/Types_of_Literacy_ed.pdf Accessed May 25, 2022.

[92] Valsts aizsardzības mācības un Jaunsardzes likums: Latvijas Republikas likums [National Defense Training and Youth Guard Law: Law of the Republic of Latvia]. 22 December 2020. Latvijas Vēstnesis, 247A. available https://likumi.lv/ta/id/319794 Accessed March 24, 2022.

[93] Ventre, D. (2016), Information Warfare. [ebook] 2nd Edition. London: Wiley, available https://www.perlego.com/book/992864/information-warfare-pdf Accessed February 3, 2022.

[94] Williams, C. (2005), "From conscripts to volunteers: NATO's transitions to all-volunteer forces", Naval War College Review, 58(1), pp. 35-62, available http://www.jstor.org/stable/26394155 Accessed 24 March, 2022.

Chapter 12 – A RISK-BASED APPROACH TO NATIONAL SECURITY – CHALLENGES AND RECOMMENDATIONS

Monica Endregard
Norwegian Defence Research Establishment
NORWAY

12.1 INTRODUCTION

The Phase I national case studies identified several themes and shortfalls of implementing comprehensive defence concepts. The Norwegian case study pointed to challenges related to protective security work and national security in light of increasing civil-military interconnectedness through globalisation and digitalisation of infrastructures and services [4]. The Norwegian Total Defence, including the Armed Forces, are subject to profound changes, both technological, structural and organisational developments. The new national security legislation was launched in 2019 to keep up with these developments. It includes modern risk management principles and shifts the balance form a predominantly rule-based regime to a risk-based approach in which mission critically should guide identification and prioritisation of security measures to achieve an appropriate level of security. Such a risk-based approach to security is nothing new. In the private sector, risk-management and risk-based approaches to safety and security have been an integral part of enterprise risk management for decades. What is new, is the shift towards such a regime in the defence sector. This chapter addresses what the national security regime implies, why implementation is challenging, and proposes a path forward.

The structure of this chapter is as follows: Section 2 presents the background and rationale for the Norwegian Security Act, and the systematics and requirements put forth by the Security Act. Section 3 addresses the characteristics, advantages and disadvantages of a rule-compliance versus a risk-based security regime. Section 4 focusses on the implementation of a risk-based security regime. It includes a hierarchy of national security values, addresses risk related concepts and what processes of risk management and risk assessment entail. Section 5 discusses implications and challenges for the defence sector. Section 6 concludes and proposes a path forward to develop improved approaches to assess and govern national security risks and achieve an appropriate level of security for the national defence, in a comprehensive defence context.

12.2 THE NORWEGIAN NATIONAL SECURITY REGIME

This section presents the main features and requirements of the new Norwegian Security Act.

12.2.1 Background

National security entails the nation's ability to uphold national security interests, encompassing sovereignty, territorial integrity, democratic governance and other national security interests (Ref. [16], p.71). The main purpose of the national defence is to create national security, peace and stability for the state, the population and society. The Norwegian defence concept comprises three mutually dependent elements: national defence capacity, collective defence through NATOs defence plans, and bilateral support and reinforcement plans. Civil-military cooperation in the framework of the Norwegian total defence concept underpins all three elements, and is crucial for strengthening societal resilience and reduce vulnerabilities (Ref. [16], p.11). A comprehensive approach is thus of key importance for securing the nation against external and internal threats.

National security interests should be protected against intentional acts that directly and indirectly may harm such interests. The purpose is to protect critical information, information systems, objects and infrastructures through measures reducing risks to an acceptable level. The Security Act and associated regulations provide the legal requirements of protective security work. A new Security Act entered into force on January 1, 2019, [7]. The reasons for substituting the law from 1998 were pervasive changes the last two decades concerning threats, security, technology and society. The intention was to create a law that is better adapted to current threats and the dynamic nature and interconnectedness of contemporary society.

The new regulation regime entails a shift from a predominantly rule-compliance approach to national security towards a regime in which risk-management is emphasised. The law is a so-called "functional law", which means that it puts forth requirements for what security condition that shall be achieved, but not how to do this. The act requires a risk-based approach as the basis for the development of appropriate level of security for organisations performing activities and operating information systems and infrastructures of importance for national security [7].

The new law thus places more responsibility on entities regarding risk and security management than the previous regime, including higher demands concerning experience and competence within protective security work. It is not straightforward to answer the questions: What level of security is sufficient? What security measures will ensure this appropriate level of security? This has proven challenging in practice, also within the defence sector. This chapter seeks to explain challenges, as well as propose a path forward, for implementing the security regime in a comprehensive defence context. Although the point of departure for this chapter is Norway, the advantages and challenges of a risk-based approach to security is probably also relevant for other nations.

12.2.2 The Purpose and Systematics of the Security Act

The Norwegian Security Act sets clear requirements for entities' security management. The Security Act with regulations stipulates that *an appropriate level of security* must emerge from value-based risk assessments. The entity itself is responsible for achieving and documenting a sound level of security. This is in principle different from the previous regime of the Security Act of 1998, which can be characterised as predominantly a rule-compliance regulation regime in which the authorities set detailed regulations and concrete requirements. The new security regime requires a change in both knowledge and management in order to develop an approach that meets modern security principles.

The purpose of the Security Act is to help:

a) Protect Norway's sovereignty, territorial integrity and democratic system of government, and other national security interests.

b) Prevent, detect and counter activities which present a threat to security.

c) Ensure that security measures are implemented in accordance with the fundamental legal principles and values of a democratic society.

(Security Act § 1-1 Purpose)

The national security interests are divided into the following five categories:

- The activities, security and freedom of action of the highest state bodies.
- Defence, security and emergency preparedness.
- Relations with other states and international organisations.
- Economic stability and freedom of action.
- The basic functionality of society and the basic security of the population.

(Security Act § 1-5)

The Ministry of Defence (MOD) states that the second category "defence, security and emergency preparedness" includes the Armed Forces and the defence sector with supporting functions in a total defence context (Ref. [6], p.34). Today's defence is directly dependent on civilian input factors from civilian total defence actors, including in the field of electronic communications and power supply. Such infrastructure and services are therefore fundamental to military operational capability.

The MOD emphasises that the Security Act provisions will also apply to infrastructure and services that do not directly support the Armed Forces, but are crucial for civil society to function and thereby important for overall preparedness and protective capabilities (Ref. [6], p.35). This entails a "limited extension of the scope of the law" as compared with before.

Pursuant to section 1-2 of the Security Act, all ministries shall identify Fundamental National Functions (FNFs) within their areas of responsibility. The Security Act defines FNF as:

> *[…] services, production and other forms of activity that are of such importance that a complete or partial loss of function will have consequences for the state's ability to safeguard national security interests.*
>
> (Security Act § 1-5)

FNFs constitute the superstructure to identify public and private enterprises and activities that are subject to the Security Act and its provisions. Annually, the Ministry of Justice and Public Security (MOJ) used to publish the updated list of all designated FNFs in its budget bill (Ref. [8], pp. 130-131). As of 2022, the Norwegian National Security Authority publishes an updated list on its web site. The functions span across societal sectors and include for instance "Law and order", "Food supply", "Power supply" and "Transport", and for the Armed Forces "Situational understanding", "Engagement", "Command and Control" and "Protection". We will return to the defence FNFs later.

Figure 12-1 illustrates the relationship between the purpose and scope of the Security Act, and the systematics for linking entities to the overarching national security interests via FNFs. National security interests are supported by FNFs, which in turn are supported by entities that are crucial to the functions.

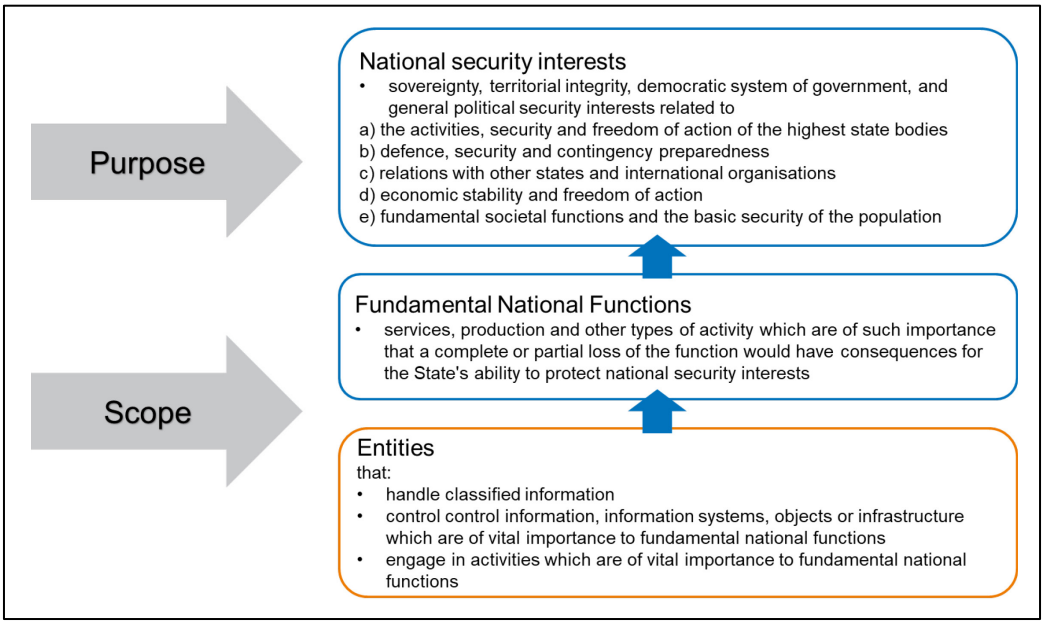

Figure 12-1: The Relationship Between the Purpose and Scope of the Security Act. National security interests are supported by Fundamental National Functions (FNF), which in turn are supported by entities crucial for the functions. The figure is based on Figure 6.1 in Ref. [6], p. 34).

12.2.3 Requirements Related to Protective Security Work

Entities of importance to national security and FNFs have legal responsibilities to perform protective security work. The head of an undertaking, or the Chief Executive Officer (CEO), is responsible for protective security work and for establishing security management as part of the undertakings' management system (Security Act § 4-1). In addition, it is a provision that:

> *The undertaking shall ensure that employees, suppliers and contractors have an adequate understanding of risks and security.*
>
> (Security Act § 4-1)

Furthermore, the Security Act sets requirements for risk assessments. Hence, the company must have the ability and capacity to continuously make comprehensive risk-based assessments based on consistent value assessments as a basis for various forms of security measures (Security Act § 4-2). The law states that:

> *Undertakings shall implement such protective security measures as are required to ensure an appropriate level of security and reduce the risk associated with activities which present a threat to security.*
>
> (Security Act § 4-3)

The entity must continuously document risk and value assessments used as a basis for implementation of various forms of security measures (Security Act § 4-4). Furthermore, there are requirements to regularly carry out exercises as part of assessing the effects of implemented security measures (Security Act § 4-3).

The law requires asset-based risk assessments; based on the premise that security, and not least the cost of security, must be adapted to the value the system or infrastructure has for the users or owners of the system. Regulations describe general requirements for how agencies and companies must assess and manage risk in order to protect their assets. Critical national assets encompass four types: critical national information, critical national information systems, critical national infrastructure and critical national objects.

Section 12 of the Security of Undertakings Regulations [9] states:

> *When an undertaking assesses risk, it shall take into account:*
>
> *a) The importance of the undertaking's critical national assets to fundamental national functions or national security interests*
>
> *b) To which activities presenting a threat to security the critical national assets may be exposed*
>
> *c) The probability that activities presenting a threat to security may arise*
>
> *d) Which vulnerabilities are associated with the critical national assets*
>
> *e) The consequences for the critical national assets of activities presenting a threat to security*
>
> *f) To what extent the undertaking is dependent on other undertakings for its proper functioning.*
>
> *The need to prepare a new comprehensive risk assessment shall be evaluated annually.*
>
> *If changes are planned, implemented or arise which may have a material effect on critical national assets, the undertaking shall assess what risks are associated with the changes.*

In conclusion, the Security Act prescribes risk assessments and risk management to protect critical national assets underpinning national security interests. The emphasis on *risk-based assessments* to obtain an *appropriate level of security* constitutes a shift from previous practices regarding protective security work. The practice of detailed prescriptive rules to ensure sound security measures dates back to days of the Cold War, but was also practised under the Security Act of 1998. The shift in Norway from a rule-based regime towards a

more analytical approach has emerged gradually, as Heyerdahl points out [12]. In 2010, the National Security Authority, the Police Directorate and the Police Security Service jointly issued guidelines for protection against terrorist acts based on risk assessment [10]. The object security legislation passed in 2011 emphasised a risk-management approach [5]. In the aftermath of the 22 July 2011 terrorist attacks in Oslo and at Utøya, Standard Norge issued a new series of standards especially developed for management of security risks.

However, overall, the previous practices of security governance leaned more on pre-defined checklists and rules, leaving organisations with less flexibility to decide on protective security measures. The 2019 national security legislation entails a shift of balance from predominantly a rule-compliance regime towards a risk-management regime. But what does this mean? The next section first presents concepts of risk, and then the characteristics, advantages and challenges associated with such regimes.

12.3 CHARACTERISTICS OF RULE-COMPLIANCE AND RISK-BASED SECURITY REGIMES

Authorities as well as organisations are currently struggling to adapt to the shift of balance of the national security regime. How should organisations under the jurisdiction of the new law operationalise its requirements?

Jore and Moen have discussed the advantages and challenges with rule-based and risk-management regimes [14]. These scholars emphasise that the two regimes are intertwined and complementary strategies, so it is not a matter of deciding between the two, but to find the right balance. Table 12-1 summarises Jore and Moen's findings on advantages and challenges of the two regimes to regulate risks. It shall be noted that Jore and Moen did not study the current Security Act.

In short, in a rule-based security regime central authorities take responsibility to define the security level as well as the security measures necessary to achieve this level of security. It is a top-down approach. In a risk-based approach, security is an organisation's own responsibility, hence a bottom-up process. In this respect, the new national security regime is a hybrid version. As illustrated in Figure 12-2, the ministries have defined the national security interests, the FNFs and identified the entities for which the jurisdiction applies, i.e., a top-down process. However, when it comes to how to operationalise the appropriate level of security, this is the organisation's responsibility based on risk assessments balanced with other concerns.

An advantage of a rule-based security regime is that it lays the foundation for a uniform level of security in the nation. The downside is that it could lead to much higher security measures than needed for many entities, being both costly and inconvenient. In a risk-based regime, security measures can be adapted to the organisation at hand and adjusted to the organisation's processes and structure, thus potentially being more cost-effective and less burdensome.

A risk-based regime opens for, and encourages, a proactive approach to security in response to a dynamic and complex "world". This is something that Jore and Moen touch upon, but does not explicitly mention. The Security Act and regulations state that the risk assessments and associated security measures shall be updated on regular basis and when changes occur. Hence, an agile, adaptive and proactive approach to risk and security is required.

The need for competency within organisations is the most important, and perhaps demanding, consequence of the new security regime and a risk-based approach. Competency includes knowledge, understanding, skills and abilities. Assessing risks require competency in several areas. The entity usually has knowledge, or the ability to produce knowledge, about its own goals, operations, assets and vulnerabilities. However, it will also need to assess interdependencies, first how the entity underpins FNFs and national security interest. In addition, it needs to assess its dependence on other organisations, infrastructures, systems and services. This requires knowledge, understanding and skills to obtain this contextual knowledge in a structured manner.

Table 12-1: Characteristics, Advantages and Challenges of a Rule-Based Security Regime versus a Risk-Management Regime, Based on the findings of Jore and Moen [14].

	Rule-Compliance Regime	Risk-Management Regime
Characteristics	• Top-down command and control-based regulatory model. • Prescriptive general regulations involving detailed, specific and often technical requirements. • Inspections by official bodies are based on checklists and imposing penalties if rules are not followed.	• Security is an organisation's responsibility. • The entity shall assess its risks as a foundation for risk mitigation through security measures. • Regulatory authorities check that the organisation has implemented measures based on risk assessments, and act more as advisors than punishers.
Advantages	• Apply to organisations across sectoral and other divides such as size, competences and experiences. • Implementation of a uniform level of security and similar security measures for critical national assets. • Easier management processes within organisations. • Simplify the inspections performed by the regulating authorities.	• Risk management is based on the organisation's own knowledge regarding its values, threats and vulnerabilities. • More focus on what to achieve, rather than the means to do so. • More flexibility on how to arrange an organisation's security regime. • Security measures can be balanced and tailor-made to the organisation giving higher cost-effectiveness and less burden. • Proactive approach to security in response to a dynamic and complex "world".
Challenges	• Rules in focus, not necessarily how to obtain an optimal level of security. • No opportunity to locally assess and mitigate risks unless it leads to higher level of security. • Detailed and stringent regulations can be problematic and burdensome. • Higher level of security measures than strictly necessary being both costly and inconvenient for the company. • Reactive responses that do not facilitate for quick regulatory changes in light of changing threats.	• The risk-management regime is no practical guide. • Presumes that the organisation knows future security risks and how to face those threats which is particularly challenging for national security risks. • Requires more efforts, methodological risk management competence and resources within the organisation. • No benchmarking for when to implement measures, thus more responsibility as well as uncertainty for the organisation.

Further, the organisations at hand need competence, including knowledge, regarding suitable and applicable methodologies and approaches to govern risk and security. Standards and guidelines are available, for instance from the Norwegian National Security Authority, International Organization of Standardization (ISO) and others. However, such standards and guidelines are often quite general and need to be adapted to the particular purpose and operationalised to be applicable in practice.

This section has compared a risk-management security regime with a rule-based regime. Norway is in the midst of shifting the balance from a predominantly rule-based towards a risk-management national security regime. What such a shift implies, is the focus of the next section.

12.4 IMPLEMENTATION WITHIN THE DEFENCE SECTOR

The remaining part of the chapter is devoted to aspects of implementing the new security regime in the defence sector and recommendations for the way ahead. First, a hierarchy of national security values has been developed, starting with the overarching political goals. This hierarchy of values constitutes a starting point for risk management and assessment, which is the topic of the subsequent section.

12.4.1 Hierarchy of National Security Values

The implementation of the new security regime requires a shift of mind-set as well as a new systematic approach that links national security interests, via military mission goals and capabilities, to security requirements and measures at a systems and technological level.

As emphasised in the Norwegian case study, the Armed Forces is a key instrument of power to protect and defend Norwegian national security interests, governance and peace and stability for the state, the population and society. National authorities have specified nine tasks for the Armed Forces (Ref. [16], p.11[1]):

1) Ensure credible deterrence based on NATO's collective defence.
2) Defend Norway and allies against threats, aggression and attacks, within the framework of NATO's collective defence.
3) Prevent and manage incidents and security policy crises with national resources, including facilitating for allied support.
4) Ensure national situational awareness in support of decision-making through surveillance and intelligence.
5) Safeguard Norwegian sovereignty and sovereign rights.
6) Exercise Norwegian authority in designated areas.
7) Participate in multinational crisis management, including peace operations.
8) Contribute to international security and defence cooperation.
9) Contribute to societal security and other key societal tasks.

These nine tasks are rooted in the national security and defence policy decisions, and lay the foundation for the national defence concept and long-term defence planning.

[1] In Norwegian, Author's translation.

The MOD has established the following five FNFs for the defence sector underpinning national security interests (Ref. [16], p.71[2]):

1) **Situational awareness:** The ability of intelligence, situational awareness and timely notification.
2) **Engagement:** The ability to handle episodes and security policy crises and, if necessary, defend Norwegian or allied territory.
3) **Command and control:** The ability to command and control Norwegian and allied forces.
4) **Protection:** The ability to protect Norwegian and allied forces, socially critical functions, as well as critical digital functions for the Armed Forces.
5) **MOD's** activities, freedom of action and decision-making ability.

The FNFs are quite general and not directly applicable for protective security work. In order to help implementation of the Security Act, the MOD has operationalised the five FNFs within its area of responsibility into twenty-four capabilities or sub-functions that offer more detail. Twenty-one of these sub-functions are military capabilities. These military capabilities serve as a unified operationalisation of both the nine defence tasks and the defence sectors' FNFs, thus forming a hierarchy linking national security values, via defence tasks and FNFs, to military capabilities. Figure 12-2 illustrates this hierarchy. The list of sub-functions (capabilities) is exempt from public disclosure, thus not specified here.

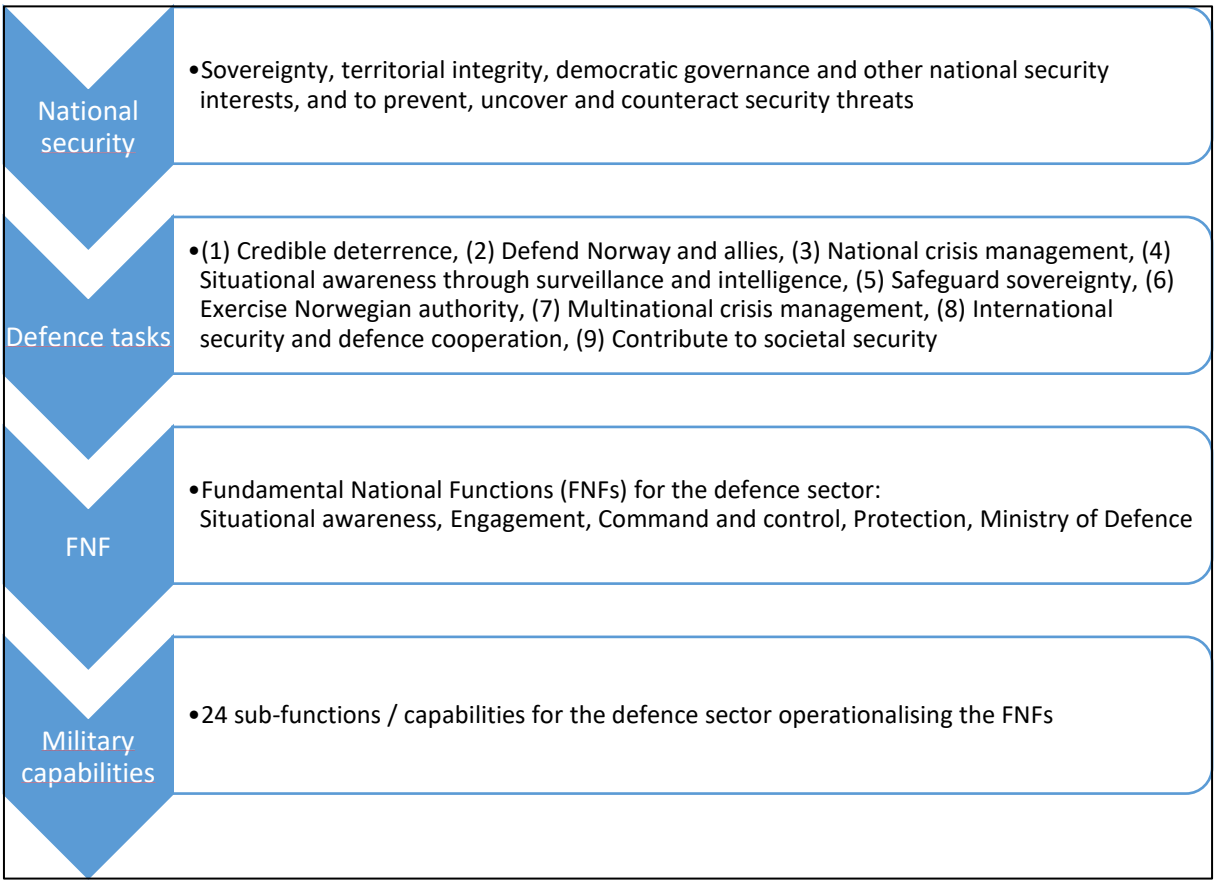

Figure 12-2: Hierarchy of National Security Values for the Defence Sector, which Links National Security Interests, via Defence Tasks and Fundamental National Functions (FNFs), to Military Capabilities.

[2] In Norwegian, Author's translation.

This hierarchy constitutes a top-down translation of the desired political national security end state to the language of military capabilities. It forms the basis for long-term defence planning and capability development, as well as security management in accordance with the Security Act. The capabilities are, however, quite general. Political guidance says what end state needs to be achieved, i.e., an acceptable level of security, but does not answer the question what needs to be done to achieve this. To answer this question, political tasks must be put in the context of military operations. Mission criticality assessments must guide identification and prioritisation of security measures. Hence, the hierarchy of national security values is the starting point for assessing risks and making decisions on security measures to obtain an appropriate level of security, as mandated by the law.

12.4.2 Key Concepts Related to Risk

In order to discuss approaches to risk assessment and management in a national security context, it is useful first to include definitions of risk and the associated concepts of uncertainty and likelihood.

Risk is about what can happen in the future. It is most common to use the term about something *negative* that can happen and the effects of that event, if no measures are taken either to prevent something bad from happening or to reduce its consequences. In the financial sector, risk is both something positive and negative. In a security context, however, the concept of risk is used about something potentially negative, which some scholars refer to as pure risk.

It can be confusing that risk sometimes, especially in everyday speech, is perceived synonymously with the probability that something can happen. The risk concept includes more. It is about how likely an event is, and also about what type, and the magnitude, of consequences an event may cause.

There is not a unified set of definitions related to concepts of risk, and some confusion about what is the concept and what is the metrics related to concepts. It is helpful that the Society for Risk Analysis (SRA) has agreed on a glossary acknowledged by a committee comprised of leading scientists within risk research [17]. The glossary represents different perspectives by presenting various definitions for some concepts. The following definition of risk has become widely accepted by the risk research community:

> *Risk refers to an uncertainty about and severity of the events and consequences (or outcomes) of an activity with respect to something that humans value.* (Ref. [2], p.8*).*

A common feature of several of the SRA definitions of risk is the emphasis on uncertainty as an integral part of the concept. The future is uncertain, thus any attempt to assess future risk is uncertain by nature. Uncertainty also stems from other sources, and is a fundamental challenge in risk assessments. The SRA expert group defines uncertainty as:

> *For a person or group of persons, not knowing the true value of a quantity or the future consequences of an activity.*
>
> *Imperfect or incomplete information/knowledge about a hypothesis, a quantity, or the occurrence of an event.* [17]

SRA distinguishes between qualitative definitions of concepts, and their measurements. One of the examples of risk metrics/description is: “The combination of probability and magnitude/severity of consequences”.

It is important not to conflate this metric or description of risk with its definition (see above). The reason for including these definitions in this chapter is that how one defines and describes risk, has practical consequences for risk assessment approaches and risk communication to stakeholders. A key point is that probability is a *measure* to express uncertainty about future events and associated consequences.

The SRA expert group defines probability (likelihood, chance, frequency) as: "A measure for representing or expressing uncertainty, variation of beliefs, following the rules of probability calculus".

SRA provides different types or interpretations of probability. Classical probability applies only for a finite number of outcomes with equal chance to occur, i.e., the throw of a dice. Frequentist probability of an event is defined as the limiting fraction of times the event occurs if the situation was repeated (hypothetically) an infinite number of times. A third type of probability is the subjective (judgemental, knowledge-based) probability, which is a subjective measure of uncertainty, conditional of the background knowledge. Frequentist probabilities are generally not applicable for security risks due to lack of relevant data [15]. Hence, knowledge-based or subjective probability are more useful in security risk assessments.

12.4.3 Security Risks

For security risks it is difficult to estimate probability of incidents. Several obstacles may occur when assessing risks associated with rare intentional threats such as terrorist actions, sabotage and armed attacks. Dillon et al. lists five challenges for terrorist attacks [3]:

- The risk is dynamic. Aggressors are strategically thinking human beings who adapt and alter modus operandi to circumvent security measures and exploit vulnerabilities.
- It is impossible to eliminate all risks due to limited available resources, thus prioritisation is necessary to optimise the cost/benefit ratio.
- The security options and the number of attack scenarios are large. It is difficult to assess the real effects of mitigating and security measures.
- The historical data are scarce leading to enormous uncertainties in estimating the risks.
- Risk-based decisions are subjective, the decision-makers trying to define an acceptable level of risk and the required security measures.

These challenges also characterise other intentional malicious acts, such as sabotage, espionage and armed attack, not just acts of terror. In particular, to evaluate and describe probabilities has proven difficult and highly uncertain for low probability/high consequence events.

In 2014, Standard Norway published a risk assessment standard specifically made for security risks, the NS 5832 [19]. The standard spurred a controversy within the broad security and safety community in Norway. The disagreements arouse from how to deal with probability in a security context [11]. Specifically, probability was not included in the risk definition, nor explicitly in the risk assessment process. The standard can be regarded as a critique of an existing standard for risk assessment from 2008, mostly used for safety risk assessments, which defined risk as a combination of probability and consequence [18]. Maal et al. (2017) found "[…] a division in the national security-debate between actors who work within the security field, and those who also work with safety related issues" [15]. The study rejected the usefulness of seeking one methodological approach for all purposes. Instead, the approach must be adapted to the case at hand, and it is the methodological knowledge and the knowledge among experts that are crucial for a sound and holistic risk assessment approach.

The controversy gradually faded. Recently, the risk and security community, under the umbrella of Standard Norge, has developed a new unified risk assessment standard, applicable for both safety and security risks, including for national security [20]. This standard does not replace NS 5832, but serves as an alternative framework.

12.4.4 The Risk-Management Process

A key principle is that risk management is the responsibility of the CEO of the organisation. In the case of the Armed Forces, the Chief of Defence holds this responsibility, which includes treating risks by implementing security measures to ensure an appropriate level of security.

What steps are included in a risk-management process? The International Organization for Standardization (ISO) issued revised guidelines for risk management in 2018 [13]. ISO defines "risk management" as "coordinated activities to direct and control an organization with regard to risk", thus part of governance and leadership. The standard further emphasises that: "The risk-management process should be an integral part of management and decision-making and integrated into the structure, operations and processes of the organisation".

This is completely compatible with the provisions of the Security Act which states that protective security work shall be incorporated into the undertakings' management system (see Security Act § 4-1).

The ISO 31000 standard outlines principles, a framework, and a process for risk management, and states that this should be an iterative process. Again, this is in line with the requirements of the Security Act with regulations (See Section 12 of the Security of Undertakings Regulations).

Figure 12-3 shows a reproduction of the risk-management process as illustrated by ISO. The process entails the following steps:

1) First, to identify the context, the goal, describing the system and its key assets, structure the process, engaging the required actors and defining key delimitations.
2) Then, to perform the *risk assessment* with its three tiered steps of risk identification, risk analysis and risk evaluation, providing the overall risk picture and recommendations on how to deal with the risks.
3) The next step is *risk treatment*. The risk assessment forms the basis for decisions on risk treatment. Are the risks acceptable, tolerable or intolerable? Risks cannot be eliminated, but must be treated by four main strategies; either avoid, reduce, transfer or accept risks.

The overall risk-management process includes recording, reporting, and communication, and monitoring and review for each step. The process is cyclic and repeated on a regular basis, or revisited due to important changes concerning the system, its assets or vulnerabilities, or the threats and hazards. The risk-management process and structure in accordance with the ISO 31000 standard is well established and widely used. The Security Act provisions, and ISO 31000 are compatible, thus the standard can be used as a framework for national security risk management.

Overall, risk management comprises balancing inputs from risk assessments with information from other processes such as cost-benefit analyses, pre-cautionary concerns and societal values such as privacy and human rights, before making decisions on how to ensure an appropriate level of security.

The risk assessment is a very important part of the risk-management process since it provides input and recommendations for risk acceptance and treatment decisions. The objectives of risk assessments are to describe the nature of risks and propose security measures. The next section provides somewhat more detail concerning the factors included, and the steps of risk assessments.

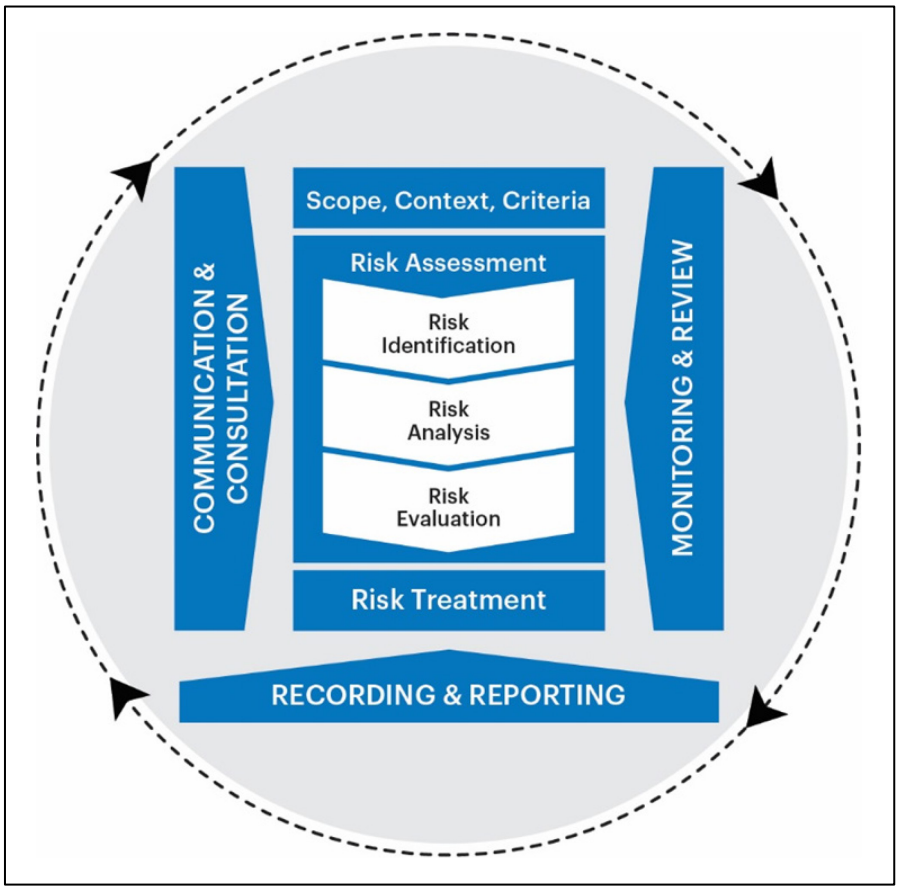

Figure 12-3: The Risk-Management Process. (Figure 4 – Process, drawn from NS-ISO 31000:2018 is reproduced by Forsvarets forskningsinstitutt (FFI) Under Licence from Standard Online AS August 2021. ©All rights are reserved. Standard Online makes no guarantees or warranties as to the correctness of the reproduction. See www.standard.no)

12.4.5 Recommendations Concerning Risk Assessment

Risk assessment is a subtask of risk management and entails identifying, characterising and evaluating risk. The aim of risk assessment is to support decision-making on risk treatment to achieve an appropriate level of security, but not prescribe what the best decision is [1].

Various risk assessment standards and guidelines exist. A previous study of several international and national standards, guidelines and recommendations for security risk assessments concluded that there does not seem to be an established and agreed "best practice" [15]. Maal et al. (2017) found that knowledge and understanding the methodology is of key importance, not necessarily the methodology itself, and summarised the following characteristics for a sound approach:

- Structured approach focussing on the process;
- Importance of the working group: broad composition and knowledge base;
- Being holistic and concrete;
- Builds on in-depth system knowledge;
- Communicates risk and uncertainty; and
- Transparent, traceable and reliable.

As mentioned previously, the Norwegian standardisation agency, Standard Norge, recently issued a new standard NS 5814 entitled "Requirements for risk assessment" [20]. This standard constitutes a combined guideline to encompass both security and safety risks. The revised standard reflects and builds on recent developments within risk research. In particular, it emphasises the need to analyse and communicate uncertainty.

A fundamental uncertainty in assessing future risks is that the future is unknown. The threat picture is dynamic and can change rapidly due to external factors such as international security political issues, intentions and capabilities of threat actors and new vulnerabilities actors may exploit. There is also uncertainty associated with the past, i.e., the knowledge available for the analysts. Relevant information can be historical data from real events, experiments or models. Sources of uncertainty lie in the data itself, but also that models or data may be unavailable. Analyses are often based on subjective expert assessments, which may be influenced by human factors, biases and group dynamics, and experts may disagree. Complex interdependencies and connections may characterise the system under study. Due to complexity, it may be necessary to make assumptions and delimitations that represent simplifications. The knowledge base for the assessment may therefore be incomplete and skewed. Hence, NS 5814 advocates for a systematic assessment of uncertainties and the quality of the knowledge base, and communication of these results to the decision makers.

Section 12 of the Security of Undertakings Regulations provides provisions that an organisation must take into account when conducting a risk assessment in accordance with the Security Act [9]. Based on these aspects, supplemented with recommendations from the NS 5814, the following steps can be included in a risk assessment approach for national security:

1) Objectives, requirements, system description and delimitation of the risk assessment:
    a) Describe the organisation's purpose, processes, and functions, and how these underpin national security interests;
    b) Describe the physical, organisational and administrative properties of the organisation or system to be subject for risk assessment;
    c) Assess to what extent the organisation/undertaking is dependent on other undertakings for its proper functioning.
2) Value assessment:
    a) Assess the organisation's critical assets and their importance to Fundamental National Functions (FNFs) or national security interests, based on the hierarchy presented in section 12.5.1;
    b) Identify critical functions, objects, systems and infrastructures for these critical assets, as well as dependencies;
    c) Identify risk evaluation criteria for values and assets.
3) Vulnerability assessment:
    a) Assess vulnerabilities associated with the assets, including weaknesses and dependencies, as well as existing protective measures/barriers and their effectiveness.
4) Threat assessment:
    a) Assess how the critical assets may be exposed to activities presenting a threat to security;
    b) Select a set of scenarios representing undesirable events for further analysis;
    c) Assess probabilities (if possible) for activities presenting a threat to security.

5) Likelihood assessment:
    a) Assess the likelihood of harmful events. In the cause of intentional incidents, assess the likelihood of attacks against assets, and the likelihood that the attack may be successful.
6) Consequence assessment:
    a) Assess the consequences for national security and FNFs of security threats and harmful events to critical assets.
7) Assessment of uncertainties:
    a) Assess and describe uncertainties associated with each of the above steps of the risk assessment process.
8) Comprehensive risk assessment:
    a) Based on the previous steps, analyse and describe the overall risk picture, including an uncertainty description.
9) Risk evaluation:
    a) Assess and compare the overall risk with fulfilment of the risk evaluation criteria;
    b) Suggest risk treatment options.
10) Other requirements:
    a) Document all steps of the assessment;
    b) The Security Act includes a provision to evaluate annually the need to prepare a new comprehensive risk assessment. Also, if changes are planned, implemented or arise which may have a material effect on critical assets, the undertaking shall assess and evaluate what risks are associated with the changes.

The above list is an example of steps to be included in risk assessments for national security purposes. None of these tasks is trivial. Such a general and seemingly simple list may hide the challenges one faces when performing risk assessments. In particular, uncertainty about the future as well as uncertainties emerging from lack of sufficient knowledge causes challenges. In addition, increasing complexity further complicates security work.

12.5 IMPLICATIONS AND CHALLENGES FOR THE DEFENCE SECTOR

The security tradition within the defence sector prior to 2019 can be characterised as skewed towards a rule-based regime. This applies to the various units of the Armed Forces, but also to the competent supervisory authority responsible for audits and security approvals. Entities implemented security measures based on prescriptive and detailed requirements and guidance by the Norwegian National Security Authority. The rationale was that an appropriate level of security existed if these measures were in place. This type of security management requires less resources and competence by the units than a risk-based approach. “It is just to adhere to the rules, and then we are good.” In addition, regulatory inspections based mainly on checklists are quite straightforward to conduct. Adaptation to a risk-management regime is challenging, and requires, as emphasised previously, more efforts, methodological risk management competence and resources. In light of its advantages, a wish to return to a rule-compliance regime is quite natural.

However, for several reasons, the static and reactive rule-based regime has flaws as a governmental security instrument in today’s societal context and for the Norwegian defence concept. Firstly, the Armed Forces are very reliant on purchases and partnerships with commercial actors as well as an extensive civil-military cooperation with civil and private entities in accordance with the total defence concept [4]. Secondly,

technological advances in infrastructures and services upon which the Armed Forces rely, develop at a fast pace, for instance within Information and Communication Technology (ICT). The defence sector is facing extensive modernisation and digitalisation, where strategic cooperation and partnerships with the business community will be important. For instance, the Norwegian Armed Forces is in the process of establishing a strategic partnership to use cloud technologies to achieve more efficient information sharing, interaction and consistent services. A defence policy statement regarding sourcing states the following concept: "As civilian as possible, as military as necessary". Hence, the reliance on private enterprises as service and infrastructure providers to the defence sector is increasing. An important rationale behind shifting the balance from a rule-compliance towards a risk-management security regime within national security is to accommodate for this dynamic organisational and technological environment.

The main objective of the Security Act is to assure that entities, public as well as private, that are of national security importance within societal functions and infrastructures, are included under its jurisdiction. This means that entities that provide vital assets or infrastructure services to the military are to be included. Some private enterprises were already included under the provisions of the old Security Act, but with the new law and regulations, an expansion to additional public and private entities is expected. Examples can be entities within important supply chains such as fuel, and infrastructure providers within electronic communication, satellite services and power supply.

In addition, the new law shall provide for a proactive and flexible regime in order to ensure that organisations continuously implement measures to uphold sound security in concert with technological and organisational changes. Technology development is moving fast. Both value chains and ownership relationships change faster than ever. The following citation summarises the situation: "Today's world is digital, complex and networked; security must address that" [21].

For the Armed Forces, this means that it is necessary to ensure an overview and knowledge of the value chains that are important for military operational capabilities, and assess risk and security implications when changes occur. This is a challenging situation, in particular, understanding and having an overview of the entities, technologies and systems the Armed Forces and other total defence actors depend upon, and weaknesses and vulnerabilities associated with these technologies and systems.

An important, though potentially challenging, Security Act provision in this context is that "The undertaking shall ensure that employees, suppliers and contractors have an adequate understanding of risks and security." (Security Act § 4-1) Hence, the Chief of Defence, being in charge of the Armed Forces, is also responsible for security and risk understanding amongst suppliers and contractors to the Armed Forces. Additional provisions apply for classified procurements (Security Act, chapter 9). With complex supply configurations for goods, services and infrastructures, across organisational and national borders, this is becoming increasingly more challenging. It is doubtful that a return to a static rule-based approach would have helped, since rules in many cases would have become obsolete before their implementation. A proactive, dynamic and knowledge seeking approach seems to be the best solution for protective security work.

12.6 CONCLUSIONS

National security entails sovereignty, territorial integrity, democratic governance and other national security interests. The purpose of the Norwegian Security Act is to ensure national security, and entities that perform activities to uphold national security fall under its provisions. This obviously includes the Armed Forces, but also total defence actors such as civilian authorities, infrastructure providers and private enterprises as part of the total defence. The Security Act and associated regulations provide the legal requirements of protective security work in these entities.

The Norwegian national security legislation from 2019 includes modern risk-management principles. The Security Act mandates all entities under the provisions of the law to ensure an appropriate level of security. Further, risk assessment shall be used to identify what an appropriate level of security is, and implement sufficient security measures. The security authorities do not answer what this level is, nor how to achieve it.

The law constitutes a shift of balance from a predominantly rule-compliance security regime towards a risk-based approach to national security. The two regimes are intertwined and complementary strategies, and the national security regime can be characterised as a hybrid version. The ministries have defined the national security interests, the fundamental national functions and identified the entities for which the jurisdiction applies, i.e., a top-down process. However, when it comes to how to operationalise the appropriate level of security, this is the organisation's responsibility based on risk assessments balanced with other concerns.

This chapter has established a hierarchy of national security values in accordance with the Security Act. Mission criticality should guide prioritisation of security measures. Security measures must underpin mission objectives and operational capability, which again are crucial for national security interests. This hierarchy is a top-down translation of the desired political end state for national security and defence tasks, down to military capabilities. It is recommended as the starting point for identification of critical functions in enterprises and assessment of critical assets to be protected. The requirement to perform risk assessments is at the core of the new Security Act. Consequently, implementation of the act requires a fundamental understanding of what risk means. In addition, it is necessary to establish methodological knowledge of risk management and assessment.

A root cause for challenges related to protective security work and national security stems from complexity caused by increasing civil-military and public-private interconnectedness through globalisation and digitalisation of infrastructures and services. This leads to increasing structural, organisational and technological complexity, and difficulty in obtaining necessary knowledge for risk assessment and management. Adaptation and development of new practices and necessary knowledge to implement a risk-based national security takes time. The only way to meet these challenges is by increasing knowledge and allocating sufficient resources to protective security work.

12.7 REFERENCES

[1] Aven, T. (2020), "Three influential risk foundation papers from the 80s and 90s: Are they still state-of-the-art?" Reliability Engineering and Systems Safety, 193:106680.

[2] Aven, T. and Renn, O. (2010). Risk Management and Governance: Concepts, Guidelines and Applications, Heidelberg: Springer Verlag.

[3] Dillon, R.L., Liebe, R.M. and Bestafka, T. (2009), "Risk-based decision-making for terrorism applications", Risk Analysis 29(3): pp. 321-335.

[4] Endregard, M. (2020), "Norwegian case study", Chapter 6 in NATO STO (2021), "Conceptual framework for comprehensive national defence system", Interim report of the SAS-152 study: Review of literature, case studies and preliminary findings. NATO STO Technical Report STO-TR-SAS-152-Part-I. Pre-release. NATO STO, Neuilly-sur-Seine, France.

[5] "Forskrift om objektsikkerhet" [English title: Regulation on object security]. https://lovdata.no/dokument/SFO/forskrift/2010-10-22-1362

[6] Norwegian Ministry of Defence (2017), Lov om nasjonal sikkerhet (sikkerhetsloven). Prop. 153 L (2016 – 2017). (English title: Act on national security (Security Act). Proposition to Parliament). (In Norwegian). https://www.regjeringen.no/no/dokumenter/prop.-153-l-2016-2017/id2556988/

[7] Norwegian Ministry of Justice and Public Security (2018), Act of 1 June 2018, No. 24 relating to national security (Security Act). https://lovdata.no/dokument/NLE/lov/2018-06-01-24

[8] Norwegian Ministry of Justice and Public Security (2021). For budsjettåret 2022. Prop. 1 S (2021 – 2022). (English title: For the Fiscal Year 2022. Proposition to Parliament). (In Norwegian). https://www.regjeringen.no/no/dokumenter/prop2.-1-s-20212022/id2875240/

[9] Norwegian Ministry of Justice and Public Security (2018), Regulations relating to the protective security work of undertakings of 12 Dec 2018 (the Security of Undertakings Regulations). https://lovdata.no/dokument/SFE/forskrift/2018-12-20-2053

[10] Norwegian National Security Agency, Police Directorate and Police Security Service (2010), En veiledning. Sikkerhets- og beredskapstiltak mot terrorhandlinger. [Guidance. Security and emergency preparedness measures against acts of terrorism].

[11] Heyerdahl, A. (2021), "Risk assessment without risk? A controversy about security and risk in Norway", Journal of Risk Research, DOI: 10.1080/13669877.2021.1936610.

[12] Heyerdahl, A. (2022), "From prescriptive rules to responsible organisations – making sense of risk in protective security management – a study from Norway", European Security, Doi: 10.1080/09662839.2022.2070006

[13] International Organization for Standardization (2018), "Risk management – guidelines", ISO 31000:2018 (E) 2nd Edition.

[14] Jore, S.H. and Moen, A. (2015), "A discussion of the risk-management and the rule-compliance regulation regimes in a security context", in T. Nowakowski, M. Młyńczak, A. Jodejko-Pietruczuk, S. Werbińska-Wojciechowska (Eds.,) Safety and Reliability: Methodology and Applications, CRC Press, pp. 677-684. ISBN 978-1-1-138-02681-0.

[15] Maal, M., Busmundrud, O. and Endregard, M. (2017), "Methodology for security risk assessments – Is there a best practice?", In L. Walls, M.., Revie, and T. Bedford (Eds.), Risk, Reliability and Safety: Innovating Theory and Practice. CRC Press. Taylor & Francis Group. ISBN 978-1-138-02997-2.

[16] Ministry of Defence (2020), Evne til forsvar – vilje til beredskap. Langtidsplan for forsvarssektoren. Prop. 14 S (2020 – 2021) ["Ability to defend – willingness to be prepared. Long-term plan for the defence sector"] (in Norwegian). https://www.regjeringen.no/no/dokumenter/prop.-14-s-20202021/id2770783/

[17] Society for Risk Analysis (2018), Society for Risk Analysis Glossary, https://www.sra.org/wp-content/uploads/2020/04/SRA-Glossary-FINAL.pdf (Accessed 17 January 2021).

[18] Standard Norge (2008), Krav til risikovurderinger. (Requirements for risk assessments). Norsk Standard NS5814:2008, (replaced by NS 5814:2021) [In Norwegian].

[19] Standard Norge (2014), Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse [Societal security – Protection against intentional undesirable actions – Requirements for security risk analysis). Norsk Standard NS 5832:2014 [In Norwegian].

[20] Standard Norge (2021), Krav til risikovurderinger (English title: Requirements for risk assessments). NS5814:2021 [In Norwegian].

[21] Weissinger, L.B. (2020), "The challenge of networked complexity to NATO's digital security", In A. Ertan, K., Floyd, P. Pernik, P. and T. Stevens (Eds.), Cyber Threats and NATO 2030: Horizon Scanning and Analysis, NATO CCDCOE Publications, pp. 236-252. ISBN (pdf): 978-9916-9565-1-9. https://ccdcoe.org/library/publications/cyber-threats-and-nato-2030-horizon-scanning-and-analysis/

Chapter 13 – BETTER-ALIGNED COMPREHENSIVE NATIONAL DEFENCE – A CHALLENGE FOR CAPABILITY-BASED PLANNING AND ENTERPRISE ARCHITECTURE METHODOLOGIES

Ivo Peets
Estonian Military Academy
ESTONIA

13.1 INTRODUCTION

Estonian security policy aims to ensure the survival of a democratic Estonian state by all internal and foreign policy means. To achieve this goal, Estonia has implemented a broad approach to security and a comprehensive approach to national defence – in addition to the military, all other areas of the state are included [4]. This wording refers to an idea called government as a whole prevalent in many Western countries. Government as a whole concept refers to integrated and unified governance, achieved through horizontal coordination between public authorities and institutions [8].

The Estonian Ministry of Defence and Estonian Defence Forces has a well-established defence planning system mainly due to its experience and integration with the NATO defence planning process since 1999 [9].

At the same time, as the Ministry of Defence and its area of government have successfully implemented NATO's capability-based planning methodology, the comprehensive approach of Estonian national defence has been arbitrarily and diffusely understood in different parts of the state system. As a result, it has been interpreted differently in various areas, which has made it difficult to harmonise inter-ministerial activities [9]. According to the Estonian National Audit Office report published in 2020, the need for unified national planning methodologies and doctrines, together I with the need to harmonise the planning methodologies of different ministries, were still relevant nearly a decade after the problem was highlighted. One of the goals of the Estonian state reform implemented at the time of writing is to improve the internal work organisation of the state, confirming that the search for suitable planning methodologies nationally is still relevant.

Estonian comprehensive national defence is based on the so-called two pillars – the primary independent defence capability and the North Atlantic Treaty Organization (NATO) collective defence [4]. In addition to the independent defence capability, the conditions for implementing collective defence must be created. The development of Estonia's military capabilities must be in line with the NATO and collective defence requirements. Interoperability is not only in the interest of a member state but is vital for NATO. As an opportunity to improve interoperability and enhance its goals, NATO has developed the NATO Enterprise Architecture Framework [12], following the example of its major member states (e.g., Australia, Canada, France, UK, USA, etc.). A methodology for dealing with complex organisations based on architectural principles.

Concepts about the possibilities of combining architectural methodology and capability-based planning appeared in the early part of the previous decade. However, although existing research refers to defence solutions, they are discarded as too industry-centric, focusing instead on alternative approaches in the private or other areas of the public sector [10], [16], [15].

Due to this, the Enterprise architecture methodology's potential may not have been best realised, which has hindered the broader spread of the approach based on the architectural methodology in the Estonian public sector.

The above gives reason to assume that the possibility of combining capability-based defence planning and NATO's enterprise architecture could be a viable alternative to research for a unified methodology in the context of a comprehensive national defence.

This chapter aims to assess whether the synthesis of capability-based defence planning and enterprise architecture methodology provides a potential solution to be used as a central planning methodology in the context of a comprehensive approach to national defence.

Consequently, answers to the following questions are sought:

1) What are the implications and requirements derived from Estonia's comprehensive national model to defence planning methodologies?
2) What are the possibilities for combining capability-based planning and organisational architecture methodologies within the framework of a comprehensive concept of national defence?
    a) What are the limitations and possibilities of a capability-based planning methodology?
    b) What are the possibilities and limitations of implementing an organisational architecture?

The question also arose as to how integrating the logic of implementing capability-based planning and organisational architecture helps improve interoperability efficiency. However, due to the limited scope of this chapter, its theoretical background was not researched.

13.2 COMPREHENSIVE NATIONAL DEFENCE CONCEPT

Traditionally, security has been most associated with the nation(state) and understood as a condition in which its people can feel safe and secure. Protected means that external pressures do not threaten the state, and internal life is characterised by the autonomy and stability of the political system. From the point of view of national defence, security management practices and culture are the first factors determining whether and how easily the country's civil, military, and other organisations can communicate with each other. Thus, the mainstay of a country's military security policy is reorganising civil-military relations to develop a system that maximises military security at the institutional level while at the same time does not sacrifice other social values.

The building of national capabilities should consider the needs and expectations of society, which highlights the need for cooperation in establishing any capability. A collaborative form of government or a broad-based approach must be defined as a process and structure in formulating and managing public policy. It connects people professionally to meet public demand through areas of government and public, private or civil activities that are otherwise more difficult to achieve. Thus, Estonian national defence is part of a comprehensive or broad approach to security (Figure 13-1) to fulfil the objectives of which, if necessary, the entire society and state resources and reserves are applied.

For example, one part of the comprehensive Estonian approach is military defence, which is to prevent military threats and, if necessary, prevent or repel them. To this end, Estonia adopts a defensive and deterrent attitude, which must be credible and based on independently developed military capabilities and collective defence [4] (Figure 13-2).

The holistic approach to national defence is called a broad concept of national defence. The strategic document for implementation is the Estonian National Defence Development Plan (ENDDP). It specifies that in addition to the structures directly providing military protection, the civil structures necessary for ensuring national security are also strongly related to national defence.

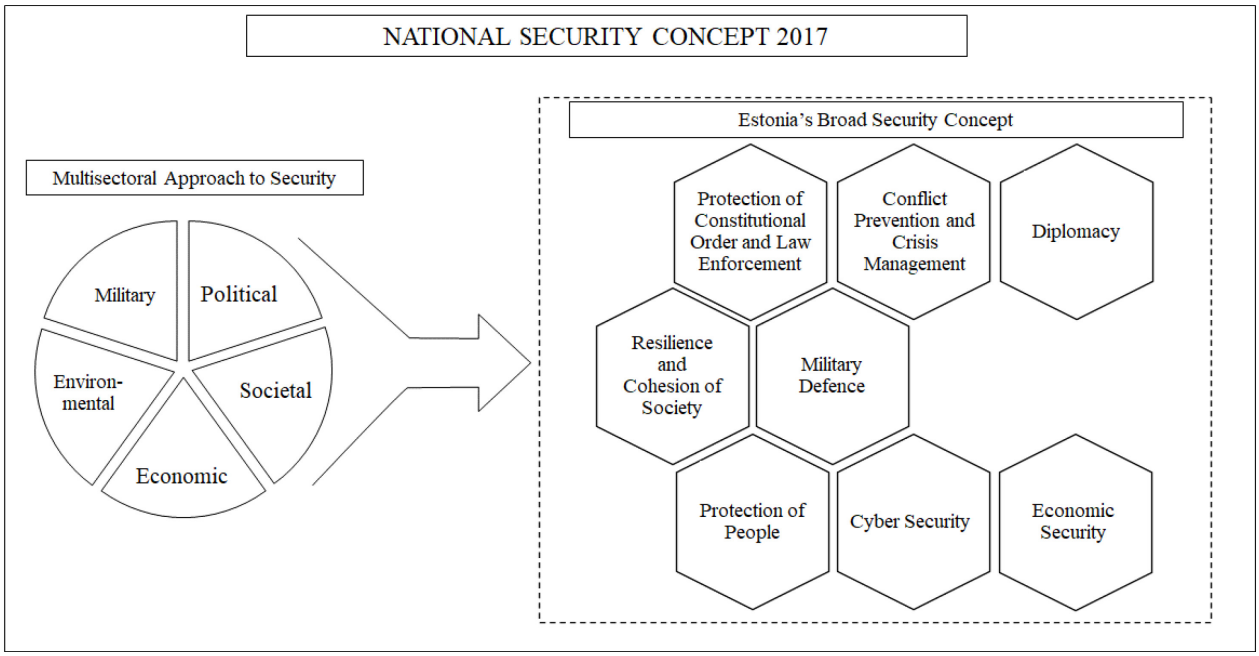

Figure 13-1: Estonian National Security Concept 2017.

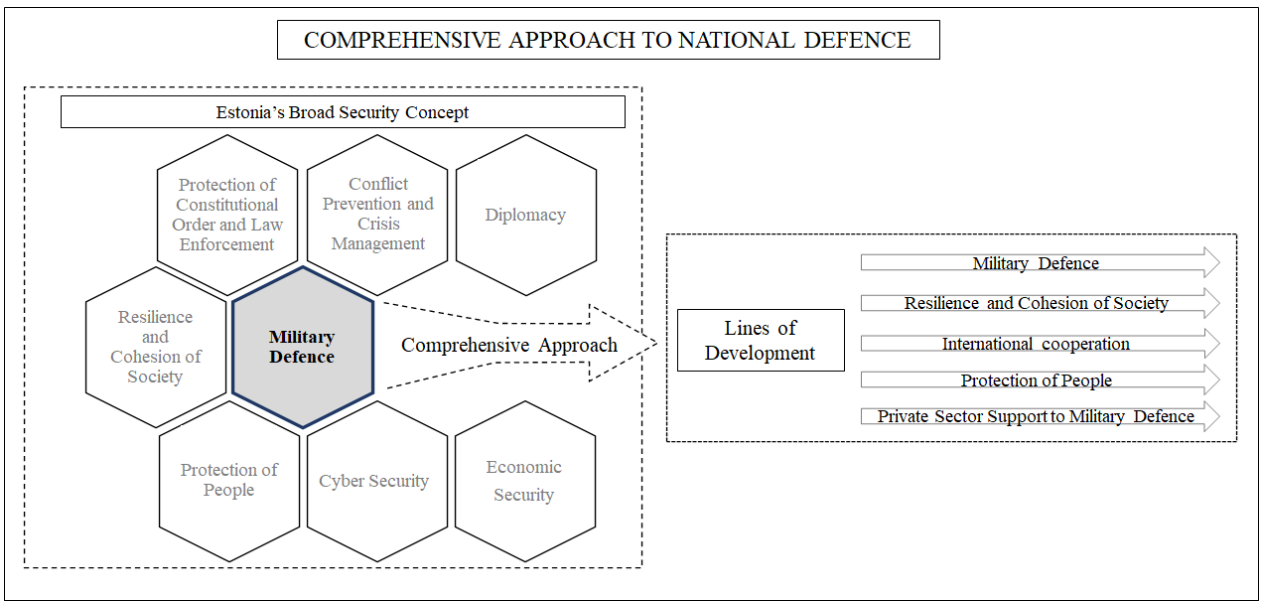

Figure 13-2: Comprehensive Approach and National Defence Lines of Development.

At the heart of the comprehensive concept of national defence is the state's defence and preparation for it. Using in an integrated manner all the capabilities at the disposal of the state, i.e., both military and non-military, and combining important activities in public, private and third sectors. The ENDDP describes national defence as a set of activities divided into six main areas of activity:

1) Continuity of the state and society;
2) International activities;
3) Strategic communication;
4) Internal security;
5) Support of the civil sector for military defence; and
6) Military defence [5].

These six lines of development are closely intertwined, forming a comprehensive concept of national defence [5]. Divided between different ministries, they connect state institutions with very different goals and tasks, creating connections that would not exist if the national defence were only based on the military aspect.

Such an approach offers opportunities and challenges – the need for cooperation between the parties increases, the requirements for coordination and the willingness to compromise, prioritising the interests of the field of national defence compared to other areas. Unfortunately, some fields still require significant improvement:

1) Improving mutual trust;
2) Harmonisation of different planning methodologies used in ministries;
3) Improving communication; and
4) Improvement of cooperation between stakeholders.

An example of the requirement to improve planning in a situation requiring real action was the Estonian autumn storm of 2019 and the resulting problems in the heavily influenced county of Võrumaa. For example, the storm disrupted or interrupted the provision of various vital services – a situation arose where the hospital manager had to drive to a neighbouring county for fuel. Not knowing that there was access to fuel and other necessary services in nearby Defence Forces Facilities and the ability to compensate for a temporary capability gap in the operation of a critical service. This situation shows how difficult it is for each case to ensure a level of awareness and cooperation between the parties that would allow the use of resources outside their organisation's scope or area of responsibility.

The problem of so-called "stovepipes" is that particular areas of responsibility and tasks limit the development of areas. The need to solve this problem has been seen as one of the priorities in the Estonian 2035 national strategy framework. It has also been considered an essential factor in the development of local government and the regional level.

Compiling the current national defence development plans aimed to avoid duplication of what was already planned in other development plans, emphasising the need for cooperation. Therefore, the capabilities are divided into non-military base and top military capabilities. The ENDDP focuses primarily on the development of top military capabilities, which is based on the threat scenarios underlying the preparation of the development plan, which are not prescribed in any other valid development plan or which exceed the usual basic need.

An essential prerequisite for selecting and developing the necessary top capabilities is a clear understanding of the basic capabilities on which they will be based. This presupposes that the ministries related to their

fields of activity and their government areas have clearly understood their contribution and role in implementing national defence. Furthermore, it is crucial for effective cooperation that the public sector stakeholders follow a unified methodology in planning. Furthermore, integrated planning is essential for better use of state and society resources and efficiency, as resolving potential security situations requires effective cooperation between many public authorities and other actors. This requires clarity in management and planning, quick and accurate decisions, and institutions with specific responsibilities and readiness to use existing capabilities and resources regardless of their affiliation.

13.3 METHODOLOGY

The present study is based on document analysis to conduct a comparative analysis and synthesis of the planning methods in focus and answer stated research questions. Data was collected from various sources: articles, publications, guidelines, legislation, development documents, etc.

There is a steady increase of literature in the field of capability-based planning, and since 2000 private sector has been increasingly looking for ways to implement it in addition to the public sector. Among authors, most references have been made to the research of Paul K. Davis, Ben Taylor and Thomas-Durrell Young, whose work is often cited and used in related articles and research.

The amount of published material on enterprise architecture is high compared to capability-based defence planning. Therefore, only articles and guidelines related to the enterprise architecture methodology were analysed from the materials related to the most common methods (e.g., Zachman, DODAF, TOGAF, etc.).

Both methodologies have been studied separately in the literature, but these methods' parallel application or combination still has room for future research. Furthermore, based on the conclusion that enterprise architecture is still a developing concept [6], the possibility of applying it more coherently with the capability-based planning method may have been overlooked. This allows the author to open the topic from a new perspective compared to previous works.

13.3.1 Enterprise Architecture

Enterprise Architecture (EA) is a relatively new field of research that aims to align the objectives of the different areas of an organisation. The concept of enterprise architecture emerged in the early 1970s when IBM began developing business systems planning methodologies. John A. Zachman is considered the pioneer of the enterprise architecture methodology.

Just as architecture in the traditional sense can concern a single building, its parts, and the whole settlement, enterprise architecture consists of several sub-components. The detailed approach and tools required to create an organisational architecture are grouped into enterprise architecture frameworks that help shape the thinking of their users. Zachman initially developed his framework specifically for IBM's information systems. This framework was named after him, published in 1987 and has been the methodology defining work since then.

To date, many different enterprise architecture frameworks have been created (TOGAF, MODAF, DODAF, etc.), the scope and possibilities of which depend on the ambitions of the compiler. However, if necessary, everyone can make a framework that suits them. To manage this diversity, different standards have been developed (i.e., ISO 402010) for standardisation and interoperability between different frameworks created based on the methodology.

These frameworks describe different business plans, processes, infrastructures, and other components as a single structured model that helps realise the vision of a structured structure. Most of these methodologies

and frameworks describe ways of representing the organisation to analyse how it is working at the moment and how it should work in the future. Organisations are very different but have similarities in their inner workings. Thus, the architecture allows visual models to describe the current and desired situation, making communication with the company's employees and external stakeholders more understandable and effective.

Zachman believes that the use of organisational architecture can help survive in the complex and changing environment of the information technology age [19]. To survive, an organisation (or nation) needs to understand the current situation, what to achieve in the future (goals), and what needs to be done to achieve it. For example, today's organisations are among the most complex systems in human history, especially in the public sector. The enterprise architecture allows an organisation to be seen as one holistic system, with multiple viewpoints to make it understandable for stakeholders and help achieve its goals [3].

13.3.2 Capability-Based Planning Methodology

Defence planning is a complex area that aims to find the forces, resources, and capabilities needed to perform various potential tasks. It is characterised by integration with more or less all other areas, is central to the public sector and is strongly influenced by legislation due to its specificities. In the following, the capability-based planning methodology is considered in the example of the field of defence, taking into account the peculiarities mentioned above in drawing broader conclusions. Capability-based planning can be divided into three stages:

1) Development of a strategic concept;
2) Development of general capability solutions; and
3) Creation of specific capability solutions.

The development of the strategic concept of an organisation must consider the tasks it is required to perform. Therefore, the first step is to find answers to several questions, the main ones being:

1) What needs to be done?
2) Where to do it?
3) When and how many times must it be done?
4) How long do the tasks have to be completed?

These issues form the so-called military outcome of defence planning [2]. To find an answer to them, the main scenarios of the threats that affect the activities of the field are prepared. Scenarios provide input for short-, medium- and long-term planning. When developing scenarios in the field of defence, the current legislation (including the Constitution) and politically expressed requirements are first considered. They are complemented by factors such as the geostrategic situation of the area, objectives and strategies, competing forces (size, type and capabilities), efficiency (training, morale, coherence, etc.), environment (landscape, weather, etc.) and the nature and likelihood of potential threats [18].

The main objective of the second phase is to analyse whether and to what extent an organisation with existing capabilities can perform the tasks defined in the strategic concepts. In the second stage, alternative capability solutions need to be developed. The development of general capability solutions deals with issues like:

1) Can the specified tasks be performed immediately?
2) How much is sufficient?
3) What are the related costs and risks?
4) What are the preferred options?

Analysing the tasks makes it possible to assess under what circumstances and which ability profiles perform well, satisfactorily (partially) or incompletely. If it becomes apparent that the tasks cannot be sufficiently performed or are entirely ruled out, the measures needed to remedy the deficiencies will be analysed. The solution may better identify the potential risks in cooperation with other institutions and assess the type and extent of irreversible risks.

To fulfil the second phase's objectives and tasks and achieve the desired results, it is necessary to involve and cooperate with various parties, not only limited to the field of defence.

The third phase (development of specific capability solutions) focuses on the cost, type and number of resources and the timing of procurement. First, planners determine the priorities the structure must fulfil in all foreseeable future situations. Followed by identifying capability gaps, i.e., areas where existing and validated capabilities are insufficient to fulfil the set core tasks. The critical question for the third stage is: how much is enough [2]? Thus, the third phase assesses what capacity is sufficient to meet the requirements derived from the different scenarios, considering the limited resources available.

13.3.3 Capability-Based Planning Process

Several process models have been developed for the practical implementation of the above. This chapter follows the process described in The Capability-Based Planning Guide by The Technical Cooperation Program (TTCP) [17].

Although other organisations have developed various solutions and explanations for the capability-based planning process, the description in the TTCP document is sufficiently general. Moreover, it does not relate to the specifics of any particular organisation, making it well suited for use in this chapter (Figure 13-3).

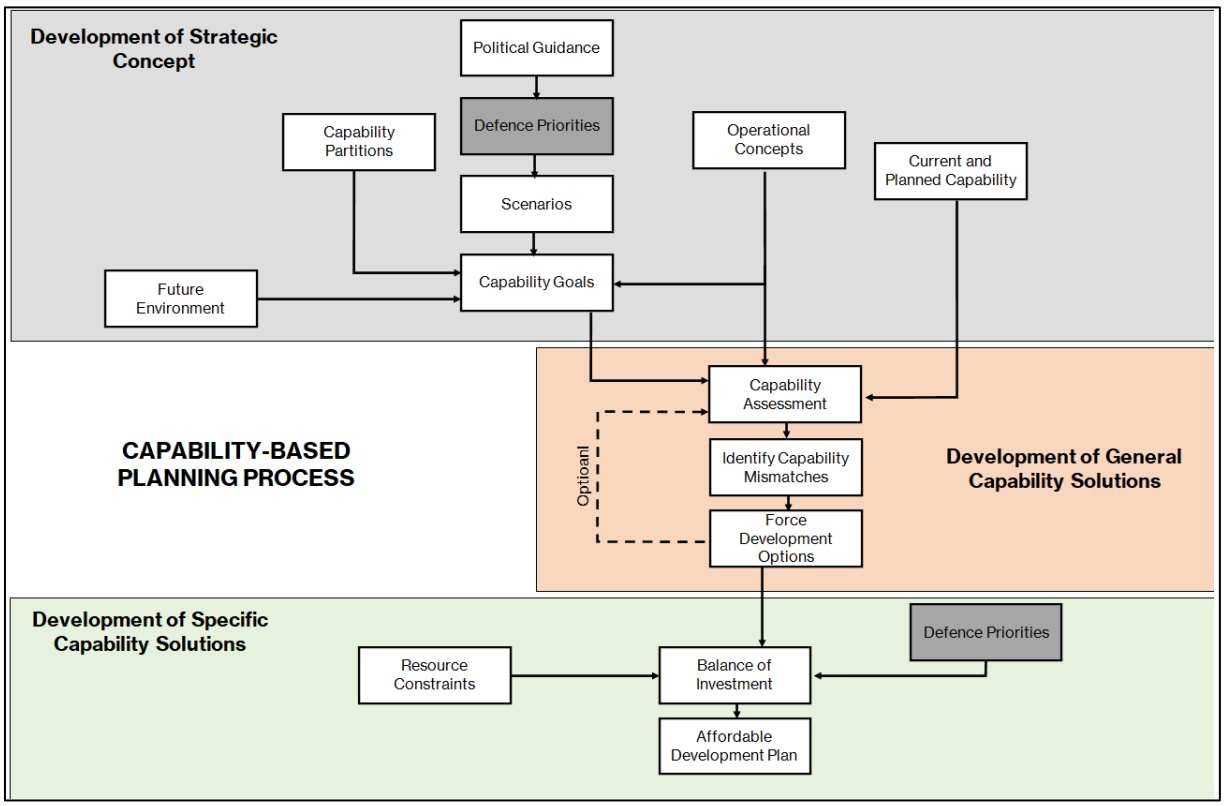

Figure 13-3: Capability-Based Planning Process.

13.3.4 Capability-Based Planning in Private Sector

Given the research objective of the chapter, the capability-based approach described by TOGAF – the private sector's attempt to combine capability-based planning and organisational architecture – deserves separate analysis, as TOGAF's capability-based approach is closely related to the TTCP process model and the theory described by RAND researcher Paul K. Davis [2].

Thus, some enterprise architecture frameworks today already aim to align the methodology with a capability-based planning process. As a result, organisations may use the capability-based planning methodology, the enterprise architecture alone, or both. However, their joint implementation is expected to lead to better results [1].

According to a study published by The Open Group in 2016 [1], TOGAF's capability-based planning process is designed to answer the following questions:

1) Should capacity be approached as unique and innovation be given priority, or should cost reductions be sought at the expense of innovation?
2) Is it a central or supportive ability?
    a) Create it or buy it?
    b) Does the organisation have sufficient resources and skills to build capacity and ensure sustainability?
3) What is the optimal rate of investment in capacity?
4) How do we find the gaps with the greatest possible negative impact, i.e., the gaps between what can be done now and what should be possible in the future?
5) Are there overlapping projects in the organisation?
6) Does it have excess capabilities?
7) Should industry standards be applied?
8) Is there progress towards implementing existing standards in this area?

The issues related to capability-based planning, their inputs and outputs form a closed circle or cycle, as in the example of TOGAF (Figure 13-4). The course of planning depends on the reason that triggered the planning cycle. The need to implement capability-based planning may arise from an entirely new organisational problem or change, for example, when a new strategic plan is outlined.

Thus, a quick comparison of the critical issues reveals a high degree of commonality and overlap. According to TOGAF, capability-based planning focuses primarily on planning and providing the necessary capabilities for a company's operations [1].

TOGAF does not divide the resolution of issues into specific phases. This should explain a closer link, especially with the private sector, where there is significantly more flexibility than the public sector, for example, in budget planning and implementation and fewer constraints due to legislation and regulations imposed by the institutions. Comparing the approaches reveals that capability-based planning is a methodology with high generalisability when applied throughout the organisation. However, this presupposes that planners have a common understanding of the capabilities nature to understand which ones are relevant to implementing a particular strategy – knowing what changes need to be made for the selected capabilities to deliver the best results for participants. The comparison result is also supported by the conclusion of other authors [11] that capability-based planning is not only a planning tool in the field of defence.

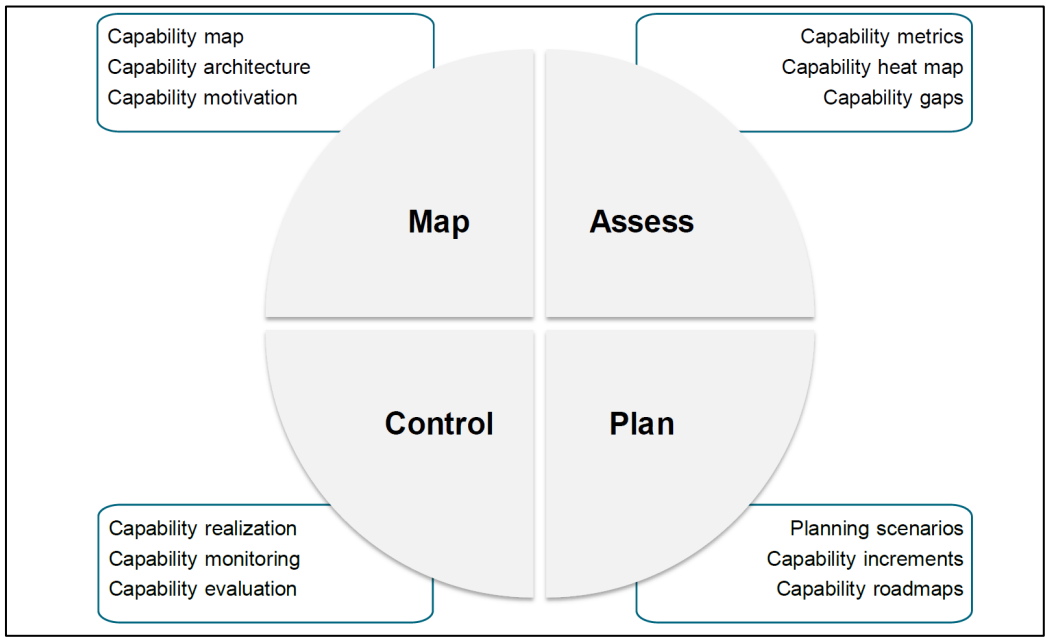

Figure 13-4: Capability-Based Planning Process Generic Activities.

The principles, tools and solutions of capability-based planning will likely be independent of the field and compatible with each other, allowing the conclusions reached in the chapter to be generalised, regardless of the approach.

13.4 CAPABILITY-BASED PLANNING AND ENTERPRISE ARCHITECTURE SYNTHESIS

As an opportunity to improve interoperability and enhance set goals, NATO has created the NATO Architecture Framework [12] – a methodology that has been implemented by its larger member states (Australia, Canada, France, UK, USA, etc.), to handle complex organisations based on architectural principles. Unlike NATO capability-based defence planning and the organisation's existing defence planning process, the use of NATO's enterprise architecture is not common in all member countries. However, it is linked to the defence planning process set out in NATO standardisation documents [13].

Thus, NATO Organizational Architecture Framework version 4 (NAFv4) will be used for future analysis. NAFv4 contains elements from the TOGAF framework and the Zachman ontology, follows the ISO 42010 standard, and is defence-oriented, thus fitting well to be used in the public sector and the broader national defence context.

13.4.1 NATO Enterprise Architecture Framework Version 4

According to NAFv4, an organisational architecture is created for an organisation, institution, company or project for various reasons. The framework supports the development of systems to meet the objectives. Thus, the architecture is created for the following reasons:

1) Plan the capabilities and transition of the organisation;
2) Achieve additional flexibility, adaptability and cost-effectiveness in capacity development;
3) Understand risks and mitigate them;

4) To achieve better adaptability in the field of activity to follow trends, changes in legislation, etc.;
5) Reconcile the company's objectives with technological priorities;
6) Plan and manage investments, control costs, etc.; and
7) To improve internal communication and broader situational awareness as a whole [12].

NAFv4 is designed and engineered to be interoperable and user-friendly. In addition, the architectures created on this basis are compatible with different standards to make use as flexible and extensive as possible. The creation of NAFv4 aimed to address the shortcomings of the traditional approaches used so far, which did not create a compatible system and resulted in cost-effectiveness, flexibility and interoperability [12].

The architecture will be designed to plan strategically, make changes, and support further analysis to identify capabilities and needs for systems development, integration, and interoperability. Architecture is a means of achieving corporate and higher-level goals (e.g., the goals of a NATO member state are related to the goals of NATO). It is a tool for the systematic management of complex organisations [12].

Figure 13-5 shows that NAFv4 is divided into enterprise architecture, system architecture, and architectural foundations. Enterprise and systems architecture regulates, within their scope, the creation and management of organisations and systems. Architecture foundations create general and pervasive links to ensure organisational and project-level architecture compatibility and interoperability [12].

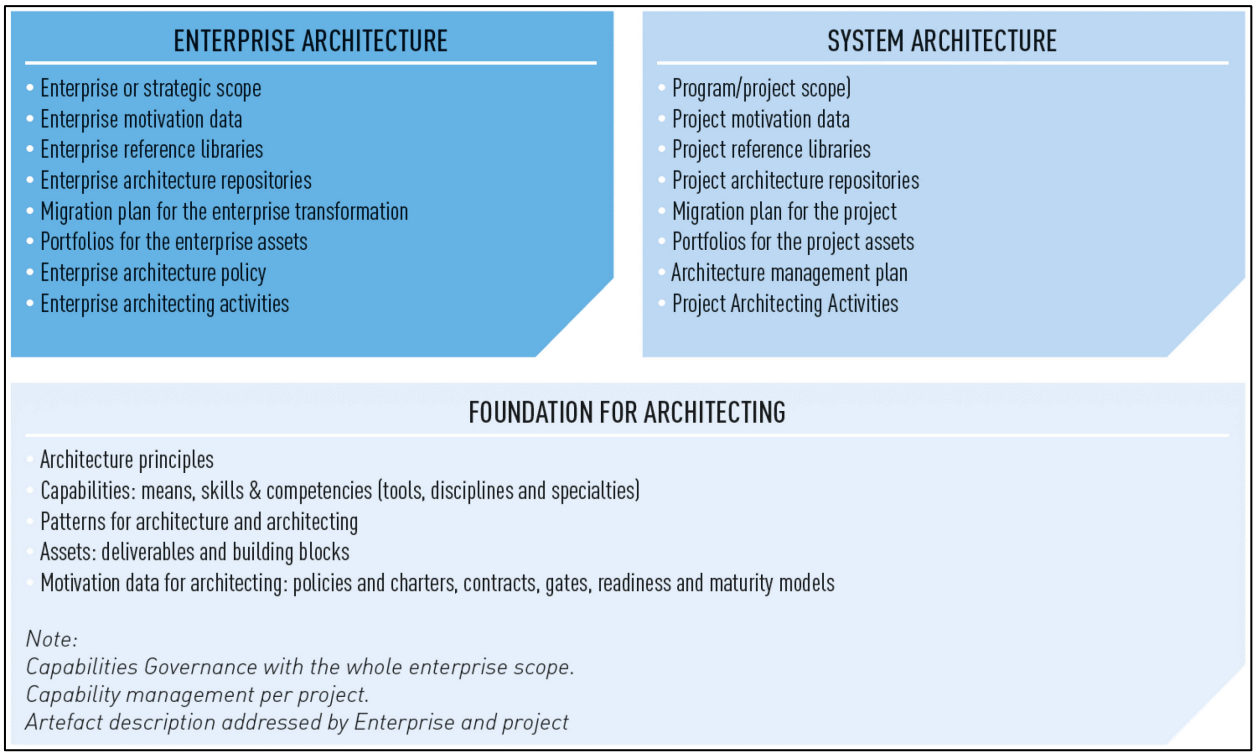

Figure 13-5: NAFv4 Main Methodological Areas.

The terms enterprise, organisation, and project used in NAFv4 have been aligned with the terminology used in this article:

1) An enterprise is where activities occur (an organisation, a company in the private and public sectors, etc.).
2) Structure shows how the company is organised, organised and structured.
3) A project is an activity aimed at creating a system, product or service that aligns with identified and available resources and requirements [12].

An enterprise-level architecture is used to make decisions that improve, for example, human and financial resources and investment across the organisation. It also helps specify the scope and functions and structure the functional activities according to the projects launched.

Project-level architecture is used to identify the resources needed for capability needs and activities (e.g., a specific military operation). The architecture makes it possible to create the equally clear links necessary for a multi-organisational project while maintaining the interoperability required [12].

An enterprise-level or project-level architecture can be a previously integrated organisational architecture. It can be linked to the architecture of one particular organisation or shared between several organisations (e.g., a single project architecture can be shared by several organisations involved in joint procurement or development of shared resources) [12].

The framework can be used to get an overview of all or part of the whole. Provided that a presentation independent of the language and tools used is identified, that helps to improve the exchange of information.

In NAFv4, information is structured according to standardised perspectives, which makes it possible to describe complex real-life problems in a simplified way (point of view). It aims to abstract the real world and reduce the complexity of real problems. This way, tools and methods can be used that would not otherwise be possible due to the complexity of the problem [12].

However, when using one architecture perspective, it must not be forgotten that several perspectives must be used simultaneously to find a complete solution to a problem.

13.4.2 Architecture Development Process

The following section analyses how the architecture is created, to highlight the connections and commonalities with the capability-based planning process described earlier.

According to NAFv4, creating architecture is divided into eight steps. These steps can be traversed in a predefined order, but the order can also be changed depending on the situation. It is also possible to go through the steps several times in a row. Information missing when the first step was taken may already be present the next time (e.g., if it is derived from a previous or subsequent step or collected from a new source). The objective defines the criteria for passing each stage, the inputs required, and the tasks to be performed to achieve the desired outputs (Figure 13-6).

When creating an architecture for the first time, it is best to go through the process in a predefined order. If the existing architecture is changed or adapted, the order of the steps can be changed as needed. This flexibility makes creating an architecture more efficient and reduces time spent on activities that are not important [12].

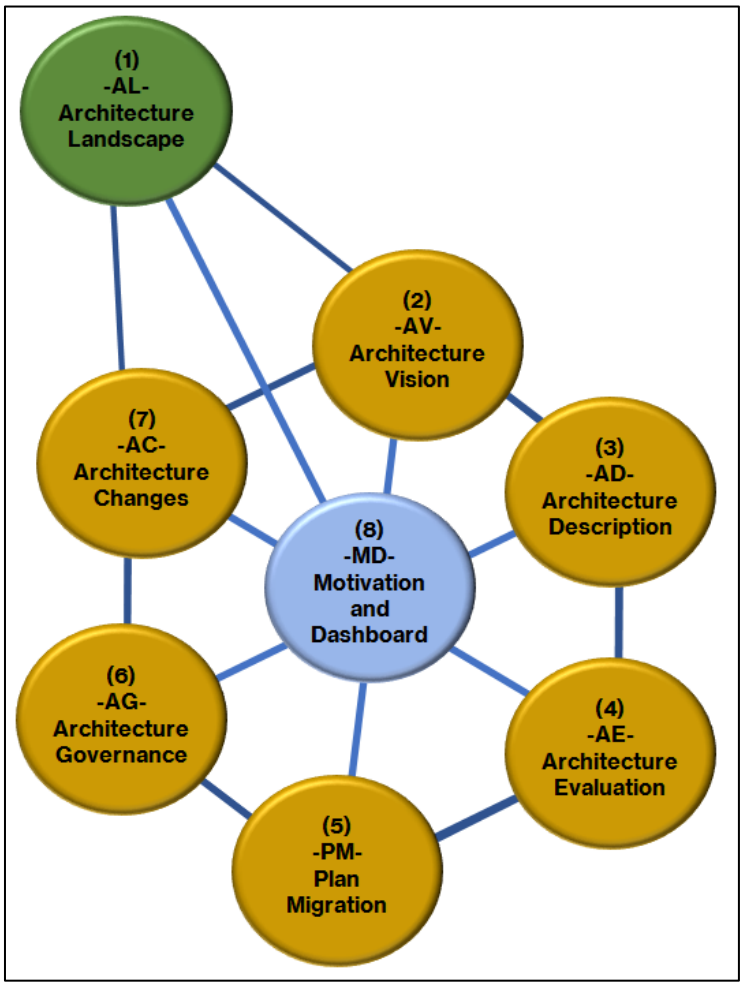

Figure 13-6: Architecture Development Process NAFv4.

13.4.3 NAFv4 Perspectives

The NAFv4 cross-tabulation (Figure 13-7) is a classification scheme that standardises NAFv4 viewpoints. It is similar in structure to the Zachman framework. Before designing an architecture, it is necessary to determine which points of view are essential for a particular architecture. If necessary, their content must be specified (Table 13-1) [12].

The viewpoint of the framework is visible in the cell where the row and column intersect. The row shows one selected entity (concept, architecture metadata, etc.) and the column aspect (e.g., taxonomy, structure, state, etc.).

Creating a new architecture based on the NAFv4 can exclude points of view that are neither necessary nor justified. Additional points of view can be added if needed to create the planned architecture. This is an essential difference from Zachman's framework (also referred by him as ontology), for example, where it is not allowed to develop additional viewpoints [19]. However, this difference does not make the NAFv4 model inappropriate or incompatible with Zachman or any other model-based architecture, but these nuances must be considered when creating a new architecture or supplementing an existing one.

Figure 13-7: NAFv4 Viewpoints.

Table 13-1: Description of NAFv4 Aspects.

Aspects	Description
Taxonomy	**Specialization hierarchies of architecture elements such as capabilities, services, etc.**
Structure	**How elements are assembled (enterprises, nodes, resources, etc.).**
Connectivity	Everything from high-level capability dependencies to detailed system connectivity.
Behaviour	How things work: • Processes - Process flows and decomposition. • States - Allowable state transitions. • Sequences - How things interact and in what order.
Information	**What information/data is used, and how it is structured.**
Constraints	**Rules that govern the enterprise, nodes, resources, etc.**
Roadmap	Project timelines and milestones affecting the elements in the architecture.

13.4.4 Relationships Between Architecture Creation and Capability-Based Planning

Next, the enterprise architecture framework and the Capability-Based Planning process (CBP) described earlier were analysed to identify their links and possible combinations. Then, a visual model was compiled (Figure 13-8). Finally, the relationships between the two methodologies were checked based on the inputs and outputs presented in the documents used for the analysis.

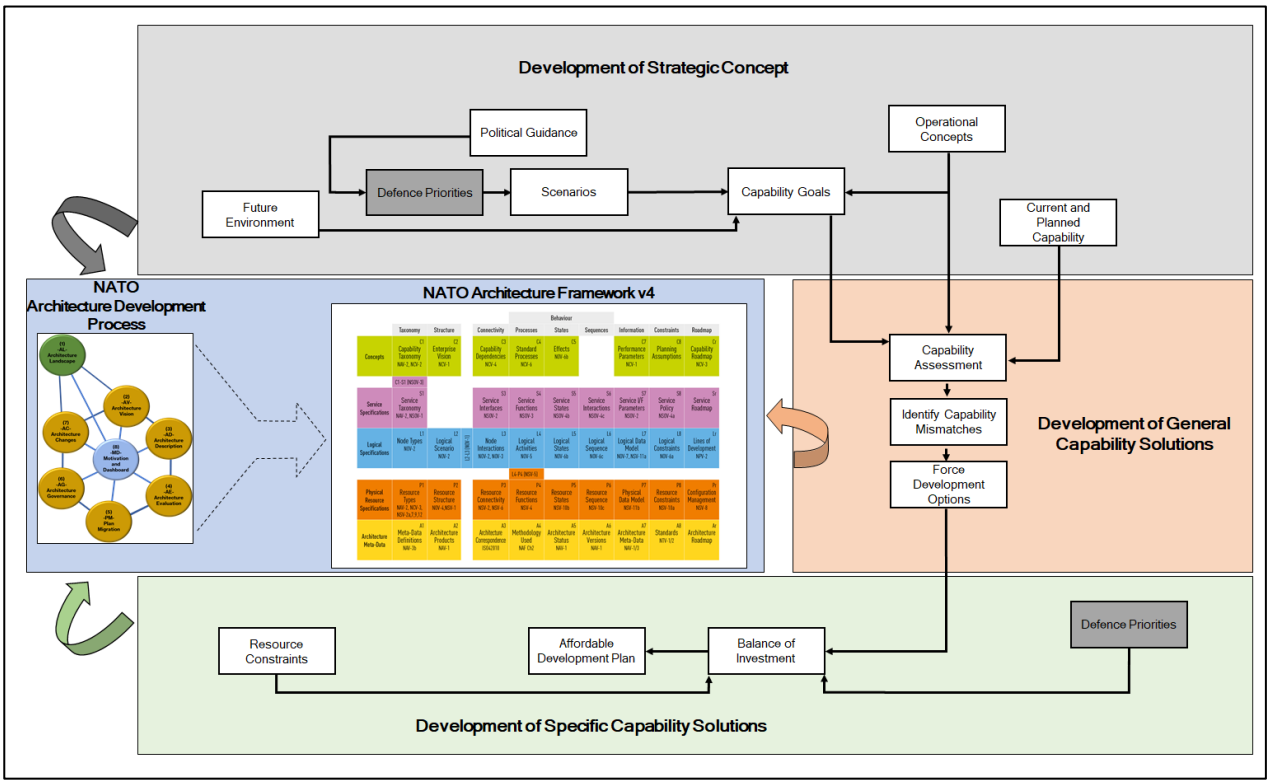

Figure 13-8: TTCP Capability-Based Planning Process and NAFv4 Architecture Framework Associations Model. Source: author.

Step 1: Architecture Landscape

Step 1 of NAFv4 can be combined with the launch of a CBP to take a holistic approach to collect raw data. The strength of a CBP is the information gathered in Phase 1 that is needed to develop a strategic concept and can be used to complement architectural perspectives. Once the scope of the organisational architecture has been determined, the scope of the CBP can also be adjusted if necessary to reduce the volume of insignificant activities. Therefore, step 1 of NAFv4 is well aligned with step 1 of CBP (Figure 13-9).

NAFv4 perspectives related to CBP phase 1: A2-A7, Ar.

Step 2: Architecture Vision

For NAFv4 step 2, at least the outputs of CBP phase 1 must be achieved, allowing the required architectural perspectives to be interpreted and the information presented to be placed in a broader context (Figure 13-10). This will help reduce miscalculations in the early stages of planning, which may be due to the excessive influence of one or the other party and may not be in line with the broader goal.

NAFv4 viewpoints related to CBP Phase 1: A1, A3, AR, P1, Pr, L1, L2, L3, Lr, S1, Sr, C1-C3, C5, Cr.

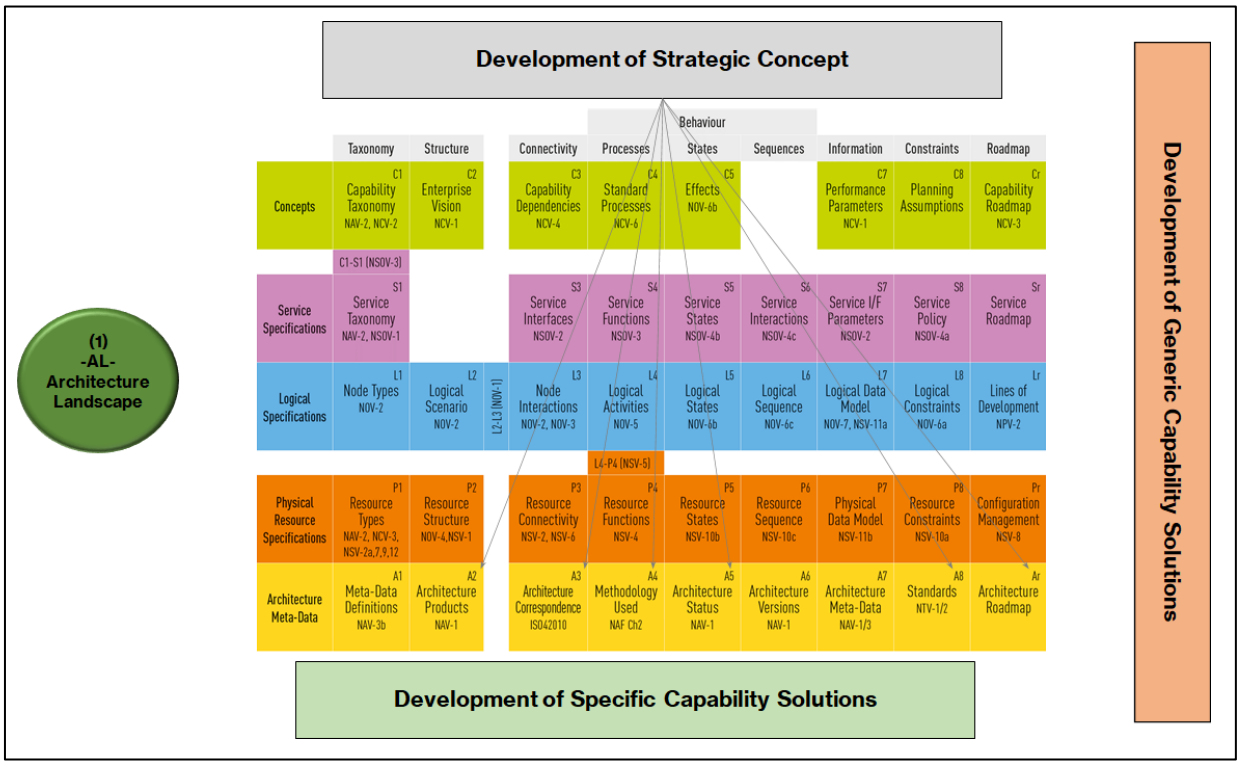

Figure 13-9: Architecture Development Step 1 and Capability-Based Planning Process Model Outputs.

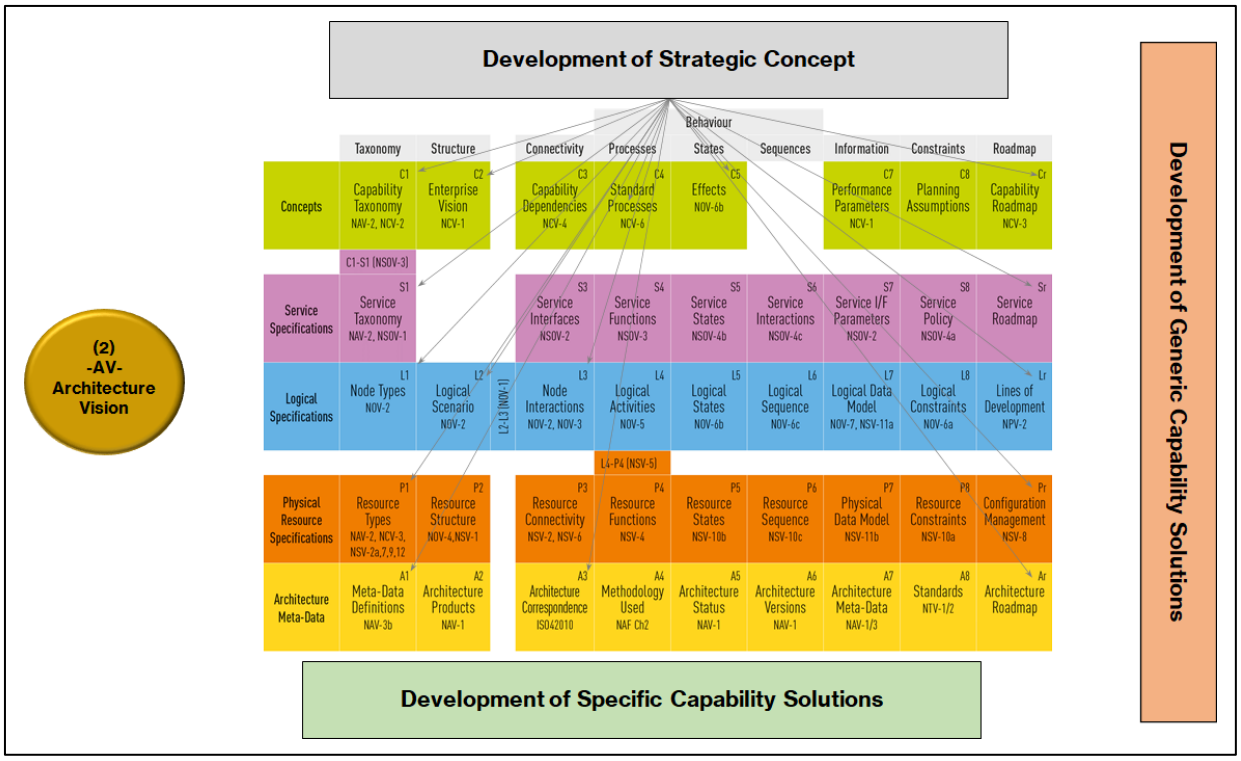

Figure 13-10: Architecture Development Step 2 and Capability-Based Planning Process Model Outputs.

Step 3: Architecture Description

For NAFv4 step 3, it would be desirable already to have CBP Phase 1 and Phase 2 outputs. However, it provides the information needed to fulfil the required architectural perspectives and the tasks identified at this stage (Figure 13-11). The three resulting commonalities between CBP and NAFv4 are presented below:

1) The capabilities identified in the CBP can be used to develop alternative architectures based on a predefined vision linked to the organisation's objectives.
2) If these capability solutions are presented as alternative structures, it is possible to systematically check whether the essential required capacities and related nuances (gaps, surpluses, etc.) have been identified during the PPP and assess how they relate to the objectives set.
3) Thanks to the architecture, the CBP results can be more comparable. Suppose the details that need further analysis are divided into systemic starting points according to the points of view. In that case, they can be forwarded to the representatives of the respective field for additional analysis. This creates previously inaccessible depth for CBP solutions.

NAFv4 perspectives related to CBP stages 1 and 2: A1, A2, A8, P1, P2, P4-P8, Pr, L2, L3, S1, S4-S7, Sr, C1-C8.

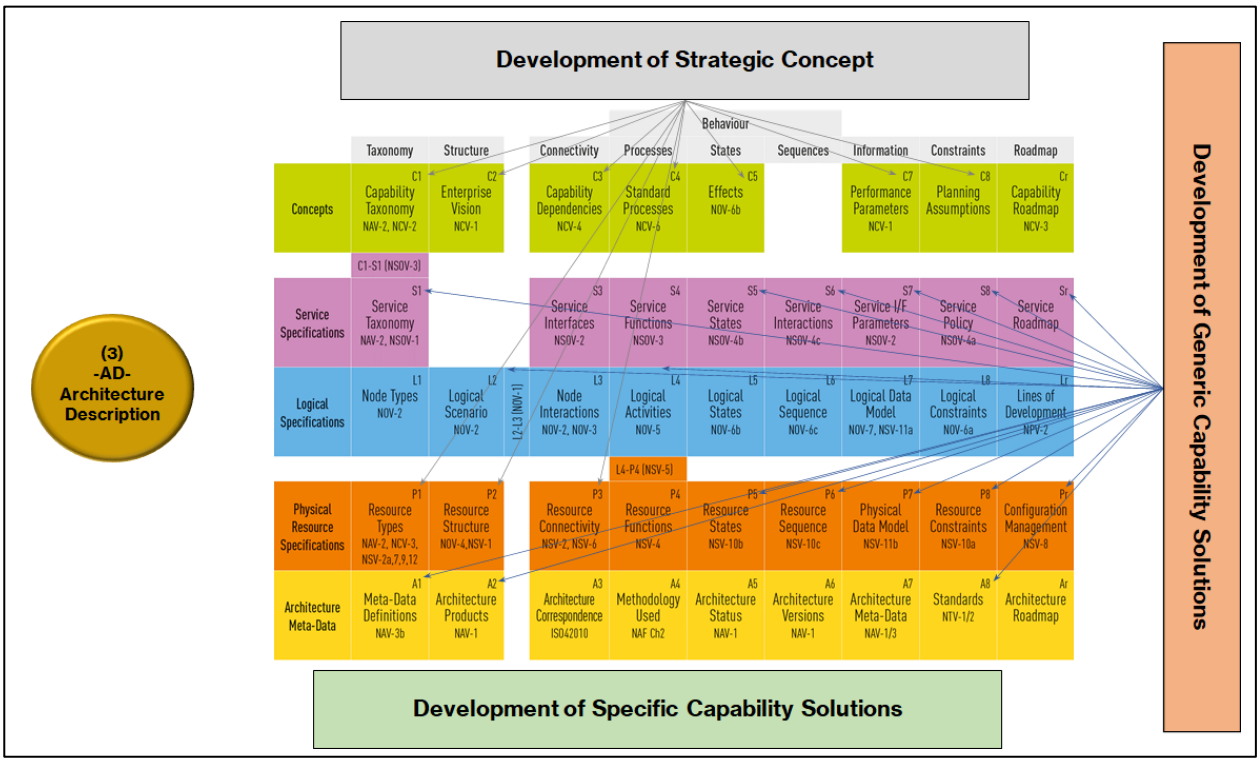

Figure 13-11: Architecture Development Step 3 and Capability-Based Planning Process Model Outputs.

Step 4: Architectural Evaluation

Unlike the previous stages, the impact of NAFv4 step 4 depends largely on whether this stage is completed before or after the start of Phase 3 of the CBP. Therefore, both options are presented below:

1) Before Phase 3 of the CBP, comparing alternative architectures developed during the previous phase allows for eliminating less promising solutions. This helps to narrow down the choices, present only the most appropriate options for decision-making (i.e., to develop specific capability options), and focus on the critical nuances. In addition, developing highly sophisticated and cross-cutting capabilities can mean significant time savings and better quality planning.

2) After the CBP Phase 3 – The results achieved during this phase may affect the suitability of the solutions already selected during the CBP and may lead to unnecessary planning costs or restrictions on the design of the architecture if the CBP results lead to decisions that are no longer changed. All in all, the most significant risk is to the quality of planning.

2) Based on the created architecture or its alternatives, it is possible to compare the prepared capabilities solutions in more detail and bring nuances to the decision-makers, which help form the positions necessary for making decisions because they are based on a holistic view. Regarding efficiency, it is best to carry out NAFv4 step 4 before Phase 3 of the CBP. This will reduce the chances of promising solutions not reaching decision-makers by diversifying planners' resources and not inhibiting the development of a holistic view across comparable solutions.

NAFv4 perspectives related to CBP stages 1-3: A2, A8, P8, Pr, L4, L6, L8, Lr, S5, S6, Sr, C1-C5, C8, Cr (Figure 13-12).

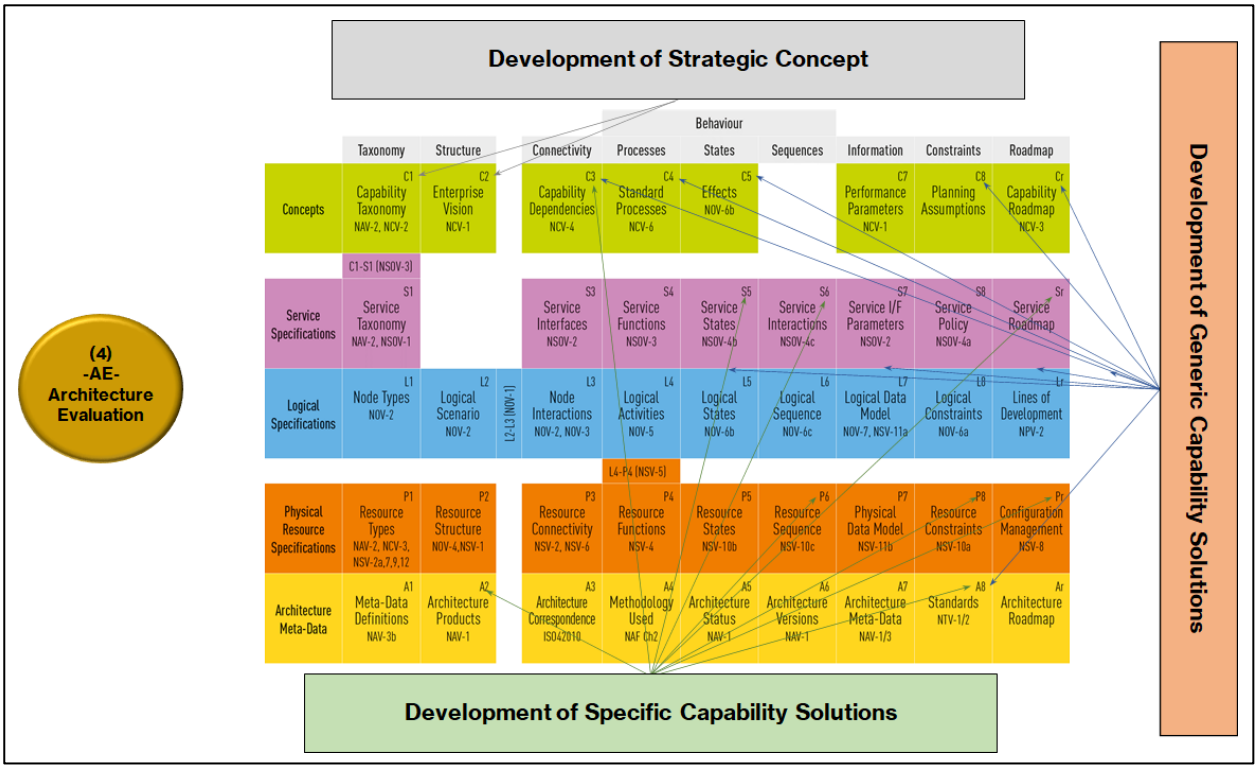

Figure 13-12: Architecture Development Step 4 and Capability-Based Planning Process Model Outputs.

Step 5: Plan Migration

NAFv4 step 5 should be undertaken after decisions on specific capability options have been made. This enables the systematic formulation of implementation plans for capability solutions, i.e., the creation of a comprehensive capability development plan, which is the main output of Phase 3 of the CBP (Figure 13-13).

This shows the most significant value of implementing the two methodologies. The planned activities can be done systematically. In step 5 of NAFv4, the transition point between implementing the two methodologies can also be seen. Whereas CBP used to play a leading role in finding the most suitable solutions to meet the vision and goals of the organisation, from the 5th step of NAFv4, the applications of capability solutions and the maintenance of situational awareness are based on the created architecture.

The author's experience shows that a plan, which meets the set goals and requirements, may not be implemented because other stakeholders withdraw from the agreement. This problem does not arise from the miscalculation of planned resources or the incompetence of those implementing the plan but rather a lack of common understanding or interpretation needed to implement the plan. Agreements may also be affected if the stakeholder's representatives change (e.g., on a rotating basis in public office positions), as this could lead to a loss of understanding of the circumstances that led to the decisions taken.

NAFv4 viewpoints related to CPB stage 3: A8, Ar, P8, Pr, L8, Lr, S8, Sr, C3, C8, Cr.

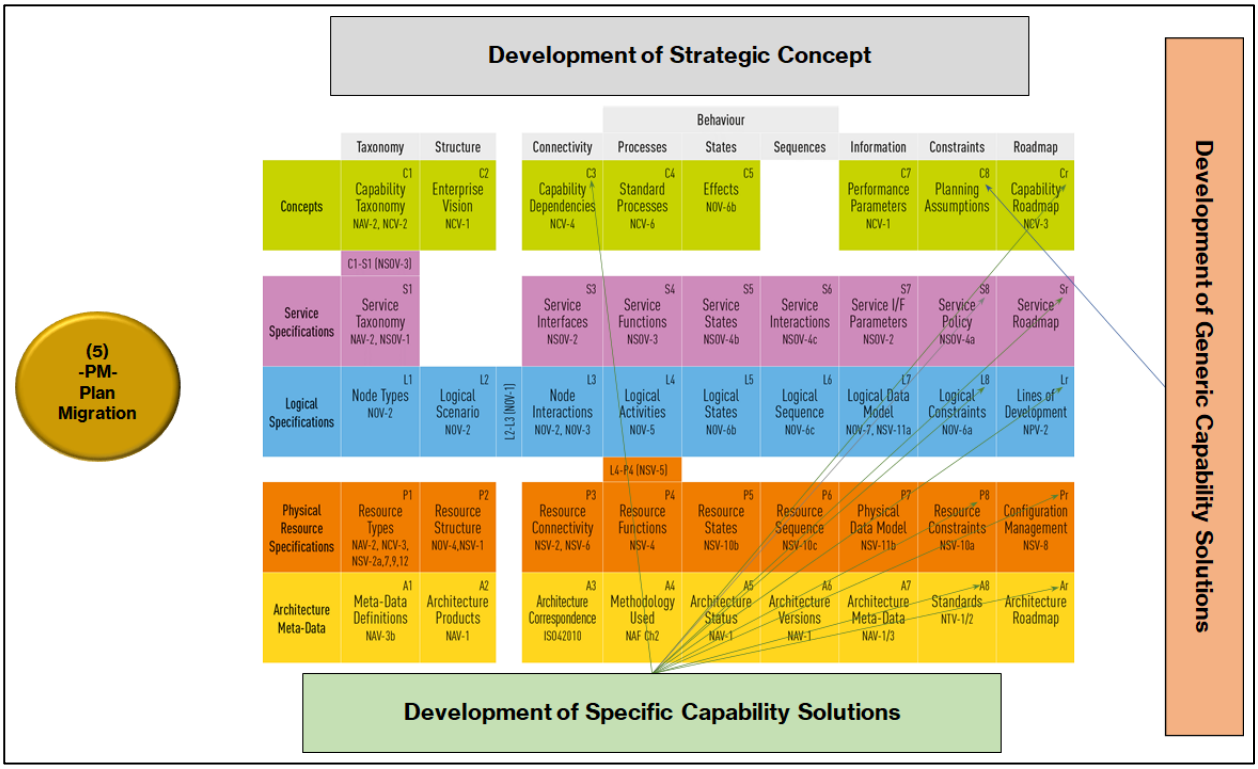

Figure 13-13: Architecture Development Step 5 and Capability-Based Planning Process Model Outputs.

Step 6: Architecture Governance

NAFv4 step 6 uses information and data previously obtained during the CBP but does not require additional planning. It is mainly the implementation of existing data in the implementation of the decided action plans, including implementing appropriate changes in the framework of the set goal. The implementation plan of the chosen capability options is specified, which is necessary to implement the capability development plan (Figure 13-14).

NAFv4 perspectives related to CPBs 1-3 step: A5, A6, Ar, P1, P2, C2.

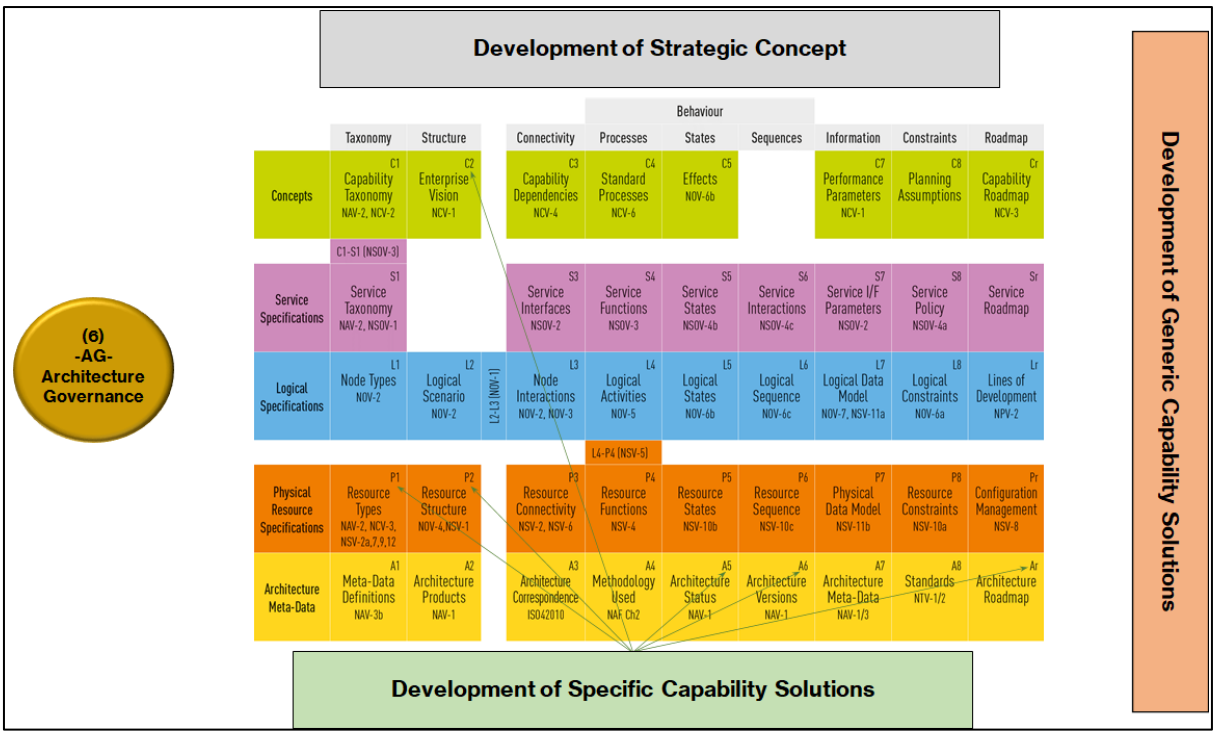

Figure 13-14: Architecture Development Step 6 and Capability-Based Planning Process Model Outputs.

Step 7: Architecture Changes

The link with the CBP develops in a situation where no specific decisions have been made on all capability options. Furthermore, no precise capability options have been deliberately chosen in terms of long-term planning (e.g., due to technology or a changing threat situation, there is not enough information to make a decision). In this situation, NAFv4 step 7 may need to develop and implement alternative solutions (Figure 13-15).

NAFv4 perspectives related to CBPs 1-3 with stages: A5, A6

Step 8: Motivation and Dashboard

Stage 8 of NAFv4 ensures that the architecture or related alternative architectures are up-to-date (Figure 13-16). From the framework's point of view, it is not a separate stage but rather an ongoing process. Hence, ensuring situational awareness of the timeliness of the architecture. The information collected in the 8th step of NAFv4 is the basis for launching the following activities.

NAFv4 perspectives related to CBPss 1-3 stage: A5.

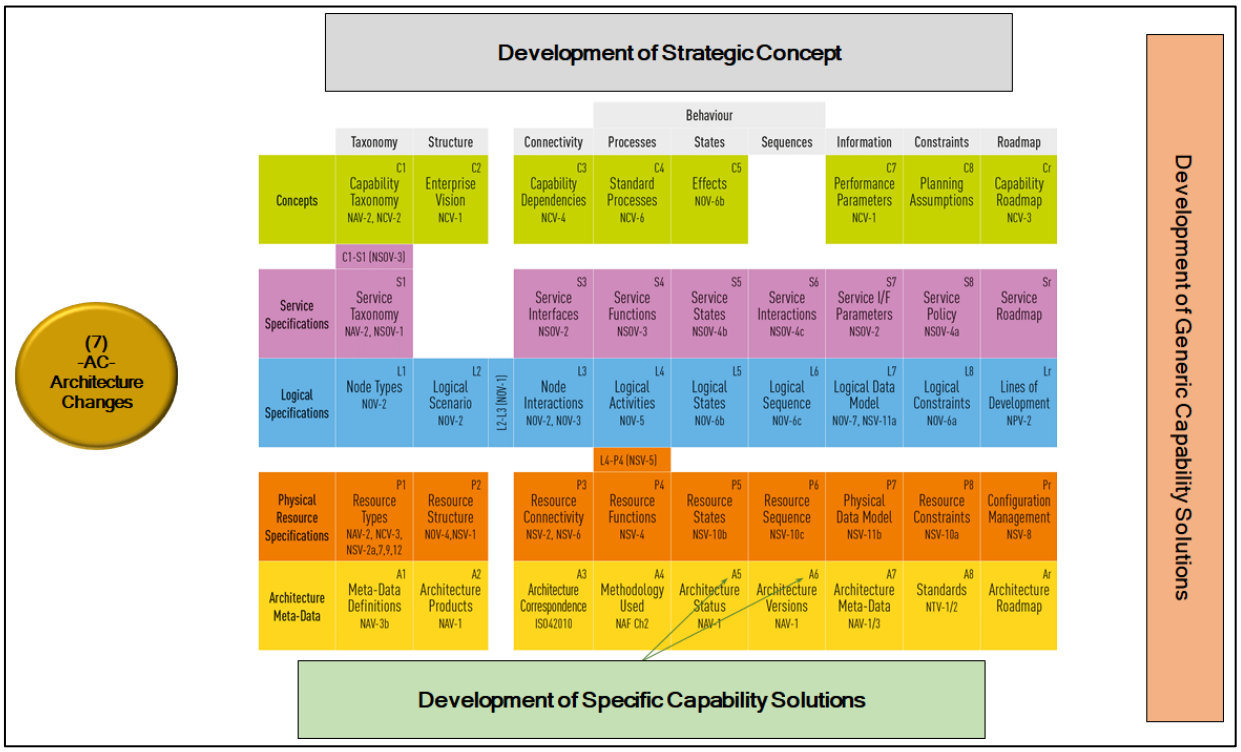

Figure 13-15: Architecture Development Step 7 and Capability-Based Planning Process Model Outputs.

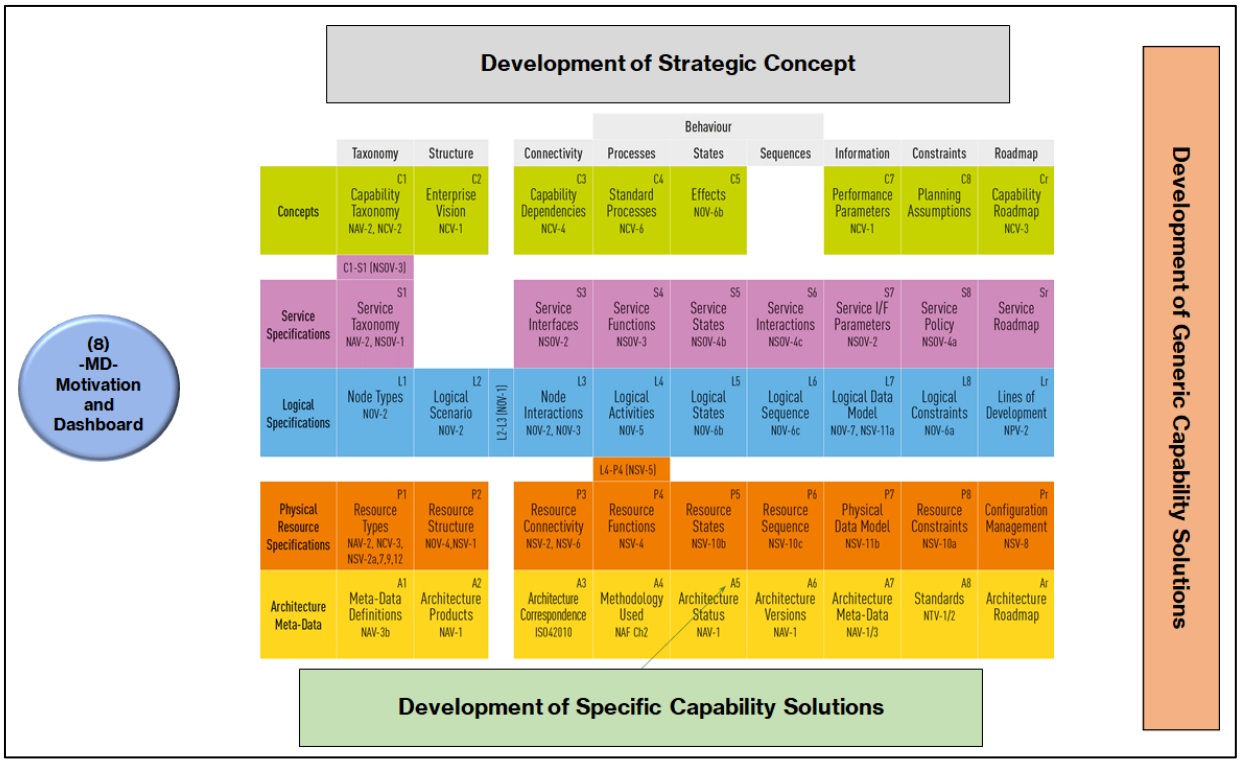

Figure 13-16: Architecture Development Step 8 and Capability-Based Planning Process Model Outputs.

13.4.5 Significant Impacts Deducted from Combining the Two Methodologies

1) **The use of capability-based planning methodologies facilitates the creation of organisational architecture.** The complexity of the methodology hinders the implementation of enterprise architecture and the time it takes to implement it for the first time. Applying a capability-based planning methodology will make reaching appropriate solutions to achieve the goal more manageable. It is relatively easy to understand and follow the general principles if there is a guide. According to the author, both methodologies must be considered complementary – with capability-based planning, optimal capability solutions can be found in the "uncertainty" for the organisation, and the organisational architecture helps to ensure the sustainability of the organisation. Based on the capability-based planning process, it is possible to choose a more appropriate organisational architecture framework and tools for the field, as those involved will have a complete picture of the organisation's capabilities (or created), including the scope and requirements of the architecture.

2) **The enterprise architecture creates the conditions for an efficient capability-based planning process.** Accurate and reliable data are needed for quality planning. The systematicity and interconnection required to produce such data is ensured once the organisation's architecture is developed in place. Appropriate capability solutions can be created through capability-based planning to fulfil the vision and goal. However, to implement these solutions or bring about change in the organisation, adequate situational awareness is needed to ensure that the chosen capability solutions remain feasible, viable and relevant in a changing situation.

3) **Using capability-based planning methodologies and enterprise architecture enables cross-sectoral capability development.** The architecture can be designed for different organisations. This helps to delimit the problem of a vast area to a reasonable extent so that the connections with the environment outside the problem remain. It does not matter whether it is a private or public institution, organisation or sector. In any case, the scope of the architecture and the level of detail based on which the problems are solved must be determined. Architectures operating at the same level can be linked to one architecture or combined as sub-architectures with one central architecture. This allows capability-based planning to reduce the number and scope of scenarios while remaining tied to higher-level (e.g., national) requirements. In the context of a broad concept of national defence, several architectures can be designed based on the set goal and the tasks set to achieve it, where connections have been created based on capabilities or fields.

4) **The cross-use of enterprise architecture and capability-based planning methodologies enhances change management and transition.** The analysis revealed that managing change and transition is one of the most crucial architecture strengths. It can be compared to building a house. If one makes a simple hut in the forest, there is no need to plan it in detail. However, it will be much more complicated if this hut is to be converted into a house equipped with communications (e.g., central heating, plumbing and electricity). The example also applies to developing organisations because their optimal development is no longer guaranteed at a particular stage without architecture. Organisations can be significantly affected by rapid changes in the overall environment. Such as the COVID-19 pandemic, which has affected all areas. When the time pressure is significant, the relevant decisions must be taken quickly. Organisations for which architecture has been created are likely to change rapidly in such circumstances, as they can immediately transition from an existing architecture to another under controlled conditions.

13.5 SUMMARY/CONCLUSIONS

The research topic of the chapter emerged from the practical professional experience that cooperation between the state's different areas of responsibility in the context of comprehensive national defence could be improved, as shortcomings in planning and shared situational awareness became evident at the stage of drafting plans. This, in turn, pointed to drawbacks in the accepted planning methodologies and possibilities

to improve the cross-sector exchange of information and cooperation by implementing uniform planning methodologies across sectors. The defence domain has for some time already successfully implemented capability-based planning principles, which led to the question of whether the methodology of capability-based planning could work for other domains as well and how this could assist in improving the coordination of their cooperation. The study confirmed that the capability-based planning methodology could be applied together with the high-potential enterprise architecture method.

The chapter's objective was to find confirmation of the above-stated standpoints. The comparative analysis of planning methods and tracing of possible faults that may emerge in their interaction indicated that capability-based planning methodology might be applied jointly with enterprise architecture methodology. This approach can potentially improve the cooperation of state institutions and raise the general knowledge of situational awareness. To reach this objective, the mentioned methodologies were analysed to discover possible weaknesses and faults in their comparison and interaction and their desired positive effects.

The chapter first discussed the architecture framework, concentrating first and foremost on problems that could be solved with the methods based on enterprise architecture. The methodology, which was worked out in the 1970s and received its contemporary form in the 1980s, is successfully used in both private and public sector for over thirty years. Even though the content and application range of the methodology and the tools, based on the architectural framework, may vary, their internal logic remains the same. They all allow handling complex organisations and their components as systematically organised elements so that important information and data are accessible to those concerned and are logically connected. This safeguards a constant overview of the organisation and its components and systematic administration of information and data, which enables it to carry out transitions, manage change and lead the organisation to achieve its goals.

After the Cold War, the uniformly defined and measurable threat disappeared, forcing the majority of NATO member states to seek new approaches to restructure their defence forces and justify expenses. Countless more minor threats replaced a single high-impact threat. As a result, it became exceedingly difficult to prove their danger and justify the necessity to work out and acquire new deterrents.

The Western Bloc countries found themselves unexpectedly in a new multifaceted hazardous environment, which forced them unavoidably to work out a contemporary defence planning methodology. The best suited for the developing situation proved to be a capability-based planning methodology that focuses on the capability requirement and does not tie planners to specific solutions at the beginning of the planning process. This approach enables one to avoid existing limitations and patterns and not to get trapped by them, fosters the development of alternative solutions, stimulates innovation and creates conditions for inter-sector cooperation.

For example, the application of capability-based planning methodology in compiling action plans in the defence field was analysed. This works in situations where it is necessary to guarantee the required competence to repel various modern threats and at the same time consider the limitations of the existing resources (incl. budgetary), which means "planning in the indeterminacy". Capability-based planning is a methodology that allows for great generalisation if applied throughout the entire organisation. The planners must have the same understanding of the essence of the capabilities to understand which are essential to implement the specific strategy. Furthermore, it is vital to understand which changes must be carried out so that the chosen capabilities may offer the best results for all those concerned.

In order to establish the possibility of using the methodology outside the defence area, it was compared with the capability-based planning methodology that is a part of the TOGAF framework. It turned out that the planning methodology principles are similar in both the public and private sectors. The differences are primarily due to the demands presented by the primary activity environments.

The author examined the possibilities of how to implement the methodologies of capability-based planning and architecture framework together, whether and how the interaction would manifest itself in the results. The analysis demonstrated that in the case of implementing the methodologies in conjunction with each other the effect is greater than implementing each methodology on their own. Each methodology focuses on establishing or maintaining the organisation, which corresponds to the vision and the set objectives. The emphasis of the methodologies, caused by their differences, showed that the methodologies rather contribute to each other than duplicate.

Capability-based planning methodology creates solutions for optimal use of existing resources and requires cooperation in cross-using capabilities. The solutions are made more comprehensively understandable for a broader range of users by including enterprise architecture methodology. Also, the capability-based solution architectures will have a more general usage in both the public and private sectors. Therefore, the hypothesis was confirmed that enterprise architecture is suitable for implementation together with capability-based planning methodology.

The overall implementation of capability-based planning methodology allows estimating the number of capabilities in different domains whose fields of application go across sectors and which can be implemented to guarantee cost-effectiveness in performing various tasks. Hence it is possible to simultaneously ascertain and compare capabilities that are needed to perform the task with currently available capabilities and, if necessary, make amendments. Implementing a capability-based planning methodology across sectors gives us a general understanding of the situation regarding all existing and required capabilities. This creates a general knowledge of capabilities that can be shared with others or cross-used to avoid unreasonable duplication. By inserting the outcomes into the architecture framework, it becomes possible to create the architecture of an organisation or domain that can help define the relations. In addition, architecture can assist in getting an overview of the current situation and drawing an implementation plan for future transitions and change.

13.6 REFERENCES

[1] Aldea, A., Iacob, M., Lankhorst, M., Quartel, D., and Wimsatt, B. (2016), “Capability-based planning. The link between strategy and enterprise architecture”, Berkshire: The Open Group. Available at: https://publications.opengroup.org/w16c

[2] Davis, P.K. (2002), “Analytic architecture for capabilities-based planning, mission-system analysis and transformation”, RAND National Defense Research Institute. Available at: https://www.rand.org/pubs/monograph_reports/MR1513.html

[3] Farahbod, R., Guitouni, A., and Bossé, É. (2013), “Towards a comprehensive DND/CF enterprise architecture methodology: A critical review DNDAF for an integrated C2 capability development”, Technical Report TR2011-022, Defence Research and Development Canada: Valcartier.

[4] Government of the Republic of Estonia, Government Office (2017), “National security concept”, available at: https://riigikantselei.ee/en/media/376/download

[5] Government of the Republic of Estonia, Government Office (2021), National Defence Development Plan 2022 – 2031, Tallinn: Estonia.

[6] Halawi, L., McCarthy, R., and Farah, J. (2019), “Where we are with enterprise architecture”, Journal of Information Systems Applied Research, 12, pp. 1-11, available at: https://commons.erau.edu/cgi/viewcontent.cgi?article=2336&context=publication

[7] Hales, D., and Chouinard, P. (2011), "Implementing capability based planning within the public safety and security sector", Defence R&D Canada-CSS-T-2011-26, available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/a555463.pdf

[8] Halligan, J., and Adams, J. (2004), "Security, capacity and post-market reforms: Public management change in 2003", Australian Journal of Public Administration, pp. 85-93.

[9] Jermalavičius, T., Pernik, P., Hurt, M., Breitenbauch, H., and Järvenpää, P. (2014), Avar julgeolek ja riigikaitse, Tallinn: International Centre For Defence And Security.

[10] Kimpimäki, H. (2014), Enterprise Architecture in Practice, Tampere: Tampere University of Technology.

[11] Murumets, J. (2007), "Renewed national defense planning and management: Capability-based planning, programming, budgeting and execution system for small states", Proceedings of the Estonian National Defense College, July 2007, Tartu University Press.

[12] NATO Architecture Capability Team (2019), Consultation, Command & Control Board, "NATO architecture framework, version 4", available at: https://www.nato.int/cps/en/natohq/topics_157575.htm

[13] NATO C3B Interoperability Profiles Capability Team (2018), NATO Interoperability Standards and Profiles, Volume 1. Allied Data Publication 34.

[14] Niemi, E., and Pekkola, S. (2019), "The benefits of enterprise architecture in organizational transformation", available at: https://link.springer.com/article/10.1007/s12599-019-00605-3

[15] Papazoglou, A. (2014), Capability-Based Planning with TOGAF and Archimate, Enschede: University of Twente.

[16] Proper, H.A., and Lankhorst, M.M. (2014), "Enterprise architecture – Towards essential sensemaking", Enterprise Modelling and Information Systems Architectures, Vol. 9, No. 1, pp. 5-21, Available at: https://www.emisa-journal.org/emisa/article/view/111/86

[17] The Technical Cooperation Program (TTCP) (2004), Joint Systems and Analysis Group, Technical Panel 3, "Guide to capability-based planning", Technical Report TR-JSA-TP3-2-2004. Available at: www.hsdl.org/?view&did=461818

[18] Young, T-D. (2006), "Capabilities-Based Defense Planning: Techniques Applicable to NATO and Partnership for Peace countries", Connections: The Quarterly Journal, Vol. 5, No. 1, pp. 35-54, available at: https://www.jstor.org/stable/26323228?seq=1#metadata_info_tab_contents

[19] Zachman, J.A. (2008), "The concise definition of the Zachman framework", Zachman International Enterprise Architecture, available at: https://www.zachman.com/about-the-zachman-framework

Chapter 14 – COMPREHENSIVE DEFENCE FOR CITY SECURITY

Erdal Arslan
Selcuk University
TURKEY

14.1 INTRODUCTION

The city has been one of the most important developments in the adventure of human existence. When we look at the definitions in the world of science, we see that the concept of city was first discussed in the East with Farâbî's "Al-Medinetü'l-Fâzıla" (The Virtuous City) and in the West with Plato's "Politeia". Again, Ibn Khaldun divides societies into Bedouin (Peasant) and Hadari (Urbanite) as an important classification. German sociologist Max Weber saw the concept of the city as a living organism and linked the emergence of modern society to urbanisation. For a place to become a city, its economy must be dependent on trade and production, not on agriculture, and must have a market, and for a settlement to gain the status of a city, there must be a defence castle, market place, city laws, courts that apply these laws and administrators elected by the city dwellers [6]. Weber divided cities into different categories within themselves; consumer cities, producer cities, agricultural cities, commercial cities, coastal cities, land cities, eastern cities, and western cities. In all of these city definitions, he said that property and personal rights with the security of the city and city law are indispensable elements in a city [13].

In this study, the issue of comprehensive defence for city security, especially including public civil cooperation, will be examined. The purpose of comprehensive defence for city security is to facilitate effective crisis management, where the population of the city is ready to defend themselves, hybrid threats to local government work during a crisis or other emergency, energy supply, health, logistics, the sustainability of city security capacity, economy and infrastructure, psychological to support critical functions of the public sector such as resistance. The goal of the comprehensive defence model for city security is to define specific defence responsibilities and the roles of local managing bodies (city top management).

Comprehensive defence activities for city security can be counted as closer defence cooperation between the private and public sectors, having courses that will increase patriotism awareness in schools, civil defence education, psychological defence education, strategic communication, economic flexibility, security unit capacity building, cybersecurity.

Following the introduction, the second part of this chapter will discuss the issue of public civil cooperation in city security. Community-Supported Policing, the importance of the neighbourhood in city security, and the inclusion of non-governmental organisations in the comprehensive defence process will be examined within the scope of this topic. In the third part of the chapter, the main subject of the study, comprehensive defence for city security will be discussed. Within the scope of this subject, closer defence cooperation between the private and public sectors, civil defence training, psychological defence training, strategic communication, and economic flexibility will be examined.

14.2 PUBLIC AND CIVIL COOPERATION IN CITY SECURITY

The concept of security is defined as security, the execution of legal order in public life without disruption, the situation in which people can live fearlessly [11].

In the framework of public civic cooperation in city security, the implementation of Community-Supported Policing, the importance of the neighbourhood for city security, and the inclusion of non-governmental organisations in the comprehensive defence process are discussed.

14.2.1 Community-Supported Policing Practice

Different policing practices are encountered in reducing crime rates. One of these applications is the Standard Model. The typical feature of the standard model can be defined as applying the laws and not focusing on a certain point. In this model, there are law practices that differ slightly about patrols for deterrence, rapid response to requests and applications made to the police, general characteristics of people, places, time, and situations (Ref. [3], p. 21). The other model is Problem-Oriented Policing. Problem-Oriented Policing is a policing model that analyses and solves crime problems. The basic idea in this model is that policing should be concerned with changing the circumstances that allow the most basic crime to be re-committed, not limited to just preventive Patrol Services and rapid response to incidents. In Problem-Oriented Policing, police must assess a wide range of issues and enforce the law when intervening in crime or misdemeanours. Besides, crime prevention efforts by patrolling certain places in areas where crime is intensively committed are less effective on crime, but more effective on disorder (Ref. [3], pp. 21, 23, 25). Another model is the practice of Community-Supported Policing. Community-Supported Policing is the accepted approach to conducting an effective security service. Community-Supported Policing is based on ensuring community participation and support in the fight against crime and implementation of security policies; primarily meeting social expectations and demands is the focus of this understanding [5].

The Community-Supported Policing model represents a broader organisational philosophy than the Problem-Oriented Policing model. Like Problem-Focused Policing, Community-Supported Policing is aimed at solving crime, but it tries to do so mostly through relationships established with community members and groups. Community-Supported Policing supports solving problems in cooperation with the society with some administrative changes, generally taking preventive action before crime and irregularity occur, and focusing more on police-public relations (Ref. [3], pp. 21, 23, 25).

When viewed from the perspective of traditional policing, a focus on high visibility and rapid response to criminal activities has been achieved thanks to a paramilitary command structure with close relations and cooperation between residents and police. In turn, Community-Supported Policing has been introduced as a new policing strategy that focuses on preventing crime by enabling officers to work with residents to solve local problems. Community-Supported Policing also strives to empower residents and improve police-community relations, goals often not emphasised under traditional policing (Ref. [1], p. 43).

Community-Supported Policing practices facilitate communication between police and citizens. This practice focuses on problem-oriented policing and can respond to the local and priority demands of citizens. This citizen-oriented orientation decreases the fear of crime by increasing police-citizen relations. A more effective Community-Supported Policing implementation requires a focus on community building and stronger collaboration with residents where it takes place. The success of Community-Supported Policing is not only measured by the high number of arrests and the rapid response to service calls (Ref. [1], p. 44).

Community Supported Police work with residents to create self-regulating, self-sufficient communities; help residents solve their own problems; develop local institutions that facilitate normative behaviour; and work proactively to solve local problems before they become crime problems. (Ref. [1], p. 45).

The practice of Community Policing is quite in line with the “Broken Window”[1] perspective theoretically and the social disorder theory more generally (Ref. [1], p. 45). According to the Broken Window Theory; “If a broken window in a building is not repaired, people who like to break Windows will think that no one cares about the building and more Windows will break, and soon there will be no windows left in the building.” This theory states that crimes are the result of loose policing practices and that tighter law enforcement policies are the primary component of promoting safer communities. In this context, if the rude words of stray young people are not taken care of, these rude behaviours can turn into serious crimes later on

[1] In this approach, it is argued that when fighting minor crimes, major crimes are prevented.

[2]. In big cities, in public places, people are most afraid of being suddenly and violently attacked by a stranger. Another source of fear is that of being harassed by people such as beggars, drunks, addicts, bully teens, prostitutes, and vagrants [7].

In neighbourhoods with poor neighbourhood relations, poor police-community cooperation, high housing mobility, and high family degradation, both formal and informal social control over residents and strangers become difficult. Lack of social control, also known as a collective activity, rudeness caused by issues such as youth grouping on the street, leads to an increase in crime, resulting in higher fear of crime and lower attachment to the local community. It has been suggested that Community-Supported Policing practice can be the address for the solution of the problems put forward by social disorder theorists. In this practice, the police can assist residents in their desire to live in a safe environment free of aggression, crime, and disorder, by working to build local institutions that promote informal social control and reduce inefficiencies even if there are no criminal problems. Empowering neighbourhood residents through institutionalisation and improving places that can be a source of crime problems can increase collective social control and people's commitment to their neighbourhoods. In the studies conducted, it has been concluded that the residents of the neighbourhoods are less afraid of crime and are less afraid of being victims than non-policed neighbourhoods due to the increase in positive relations between the residents and the police in places where Community-Supported Policing is implemented (Ref. [1], p. 45).

14.2.2 The Importance of the Neighbourhood in City Safety

It is stated in the United Nations Safe Cities Program that there is no single cause of the increase in crime, but a combination of various reasons. In this context, three main reasons have been identified. These are *social, institutional, and physical environment of the city. Social reasons*: social exclusion can be counted as the most common social cause of delinquency, depending on the reasons for long-term unemployment or marginalisation, dropping out of school or illiteracy, and lack of socialisation within the family (Ref. [12], p. 2). *Institutional reasons*: are described as the inability of the criminal justice system consisting of police, courts, and prisons to handle minor crime cases. Fighting against major crime has come to the fore in policing practices worldwide, and more attention has been paid to technology and approaches related to them. In many countries, pedestrian or bicycle police, and motor patrols with no specific targets were used in the old way of operating. Priority policing goals, such as fighting major crimes, have widened the distance between the police and citizens who have lost confidence in fighting crime. Due to the slow pace of justice, the judiciary alone (courts) is not sufficient in the development of anti-crime activities in cities and the fight against increasing minor crimes. The penalties imposed are not adapted to respond to minor violations of the law. Besides, an inefficient judicial system and a lack of accountability for crimes such as money laundering, mafia-gang participation, corruption, and human rights violations create a feeling of impunity and increase crime. Among the reasons related to the *physical environment of the city*, poor management of the urbanisation process, insufficient urban services, exclusion of security issues, the emergence of poorly protected semi-public spaces can be counted. The first consequence of the increase in crime is developing a widespread generalised and often non-objective sense of insecurity in the urban population (Ref. [12], p. 3).The second consequence of the increase in crime is the impact of insecurity on the poor. While all social classes are affected by insecurity, the poor who do not have any means of defence are more affected. Therefore, urban violence erodes the social capital of the poor, shatters their associations, ultimately hampering social mobility, especially the mobility of young people. The third consequence is the increase in total security costs. The fourth is the widespread increase of private security companies and the resulting question of how the relationship between the police and private security companies will be in terms of both action and responsibility (Ref. [12], p. 4).

The neighbourhood is defined as "each of the parts where a city is divided into a town, a sizeable village" or "all of the people who live in the parts where a city is divided into a town, a sizeable village", according to the Turkish language institution [11].

Some physical arrangements are made in the neighbourhoods to prevent crime. Crime Prevention Through Environmental Design (CPTED) strategies are one of them. Environmental Design and Crime Prevention strategies are a multi-disciplinary approach. These strategies aim to reduce the opportunities for crimes arising from the design of structures or neighbourhoods. Environmental Design and Crime Prevention strategies include a set of design principles that are brought together and adapted to local elements, related to the wider implementation of landscaping to reduce the opportunities of criminal events. Although the relationship of these principles to crime prevention in practice is clear, the human-centred qualities expected to be associated with the design elements are lacking (Ref. [10], pp. 207-208).

Environmental Design and Crime Prevention strategies have evolved in time. While most real techniques have been in use for hundreds of years, the urban relationship between the environment and criminal behaviour has only been built in the last few decades. Each of these strategies provides guidelines that can be applied to reduce the fear of crime and the scope of crime and improve the quality of life of the residents, such as a property owner, builder, or renovation. These rules are; *natural surveillance, regional reinforcement, natural access control,* and *maintenance. Natural surveillance* is a concept aimed at keeping intruders easily observable, placing physical features, activities, and people in a way that maximises visibility and is, therefore reduces the likelihood that criminal acts will be committed. The physical design within the *regional reinforcement (reinforcement)* framework can create a domain or extend the domain. Users of physical design are encouraged to develop a sense of territorial control, while potential criminals perceiving this control are discouraged. The concept of territorial reinforcement includes features such as landscape plantings, pavement designs, signs, and open fences that define property boundaries and separate private from public spaces. *Natural access control* is another design concept aimed primarily at reducing opportunities for crime by denying access to criminal targets and creating a perception of boundaries. People are physically guided to an area through the strategic design of streets, sidewalks, building entrances, landscape design, and neighbourhood passages. Design elements are very useful tools for clearly defining public roads and blocking access to private areas and structural elements. *Maintenance* allows a space to be used continuously for its intended purpose. Proper care prevents loss of visibility. However, improper maintenance can prevent landscape elements from reaching the desired environmental design and crime prevention effects (Ref. [4], p. 4).

In studies conducted in Turkey, discussions of city security concepts only dealt with and offered solutions to the traditional criminal activities, neglecting issues such as terrorism, armed conflict and attacks. In this study, however, terrorist incidents, armed attacks, or city security in case of conflict are discussed. The first of these issues is the involvement of non-governmental organisations in the comprehensive defence process.

14.2.3 Inclusion of Civil Society Organisations in the Comprehensive Defence Process

Within the scope of the inclusion of non-governmental organisations in the comprehensive defence process; The issues of “the power of civil resistance, which is the first line of defence” and “the weak points of modern cities and the risks they face” are examined.

14.2.3.1 Civil Resistance Power: The First Line of Defence

Civil resistance power refers to the individual and collective resistance of the civilian section against an armed attack. The capacity of this power needs to be maintained and developed. The main purpose here is to provide civilian support to the military (police and law enforcement) for the continuity of the administration and the provision of basic services [9].

Modern societies are a highly complex, with their integrated and interdependent sectors and vital services. This leaves them vulnerable to the danger of their system being disrupted by a terrorist or hybrid attack. These sectors are energy, health, transportation, finance, IT, water, food, public and legal order and security, the chemical and nuclear industries, as well as aerospace, which is counted as research. Terrorist and hybrid

attacks (especially recent cyberattacks) target civilians and important infrastructures, most of which are privately owned [9].

The conditions required for civil preparation can be listed as follows [9]:

- Guarantee of the sustainability of local government bodies (city top management) and vital local government services;
- Durable energy supply;
- The ability to deal effectively with the uncontrolled migration of people;
- Durable food and water resources;
- The ability to cope with mass casualties;
- Durable communication systems; and
- Durable public transportation systems.

These conditions, civil structures, resources, and the durability of the services provided constitute the first lines of defence of modern societies. In countries with higher resilience, where the public and private sectors, as well as all local government bodies (city top management), are involved in civil preparedness, there are fewer weak points that their enemies can target or leverage. Also, societies with high resilience tend to recover immediately after a crisis. Compared to societies with less resilience, they can recover much faster and return to their functional levels before the crisis. This kind of resilience would be useful in the face of threats ranging from responding to a terrorist attack to potential collective defence scenarios [9].

14.2.3.2 The Weaknesses of Modern Cities and the Risks they Encounter

Modern cities contain interconnected sectors and vital services. These cities have relied on the proper functioning of the underlying infrastructure and assume that these infrastructures can cope with any disruption that may occur. This also increases the risk of various adverse effects occurring one after another in the case that operation is interrupted. In normal times, the system appears to be working efficiently, so direct public intervention is not required. It is left to the private industry sector to eliminate the deficiencies that may arise in the supply of goods and services. However, the private sector may focus primarily on protecting their structures and minimizing their costs in case of great distress, rather than preparing for large-scale possible situations that will create a chain of negative effects on production, trade, and the whole society [9].

The level and effects of foreign direct investments in sectors such as airports, ports, energy production and distribution, and communication, which have strategic importance, especially in cities, lead to questioning the access, control, and sustainability of such infrastructures, especially in times of crisis when it is necessary to support the military [9].

Civil resistance force preparedness in cities should be made against all kinds of dangers. This preparation should include planning and preparations for natural disasters, as well as threats such as hybrid attacks, terrorism, and armed conflict (attempt). The city senior management should recognise the need for more direct cooperation with the private sector, as well as the efforts of all public institutions regarding the risks and weaknesses that will arise due to the interdependence of the sectors that meet the needs of the public. Also, civil preparedness activities should include the development of sector-specific guides and tools. In this context, it is important to make preparations that will guide a wide range of issues such as how to deal with large migrations involving hundreds of thousands of people, cyber risks faced by the health sector, comprehensive planning for events that cause mass casualties, and guaranteeing the safety of health supply arrangements [9].

14.3 COMPREHENSIVE DEFENCE FOR CITY SECURITY

Comprehensive National Defence forms the basis of comprehensive defence for city security. Comprehensive National Defence is the development of the defence system by strengthening the national and collective defence capabilities of countries to provide security and crisis preparedness in all sectors, including armed attack / conflict preparedness. The main purpose here is to improve the deterrence capabilities of countries and to develop resistance to possible crises or armed conflicts [8].

The purpose of comprehensive defence for city security is to facilitate effective crisis management, where the city populace is ready to defend itself against hybrid threats, and local government work during a crisis or other emergency to protect energy supply, health, logistics, the sustainability of city security capacity, economy and infrastructure, and provide psychological support for critical functions of the public sector such as resistance. These critical functions should be planned, coordinated, and implemented by local government bodies (city top management) in partnership with private actors, NGOs, and residents. The goal of the comprehensive defence model for city security is to define specific defence responsibilities and the roles of local government bodies (city top management). The goal here is to strive to minimise distrust and strengthen ties with the city population, the business world, NGOs, and public administration. In creating mutual trust, it is essential to bring together people with different ideas from different structures of organisation. A partnership between private entities and public authorities is equally important in establishing open personal contacts and contractual relationships. ***A decentralised system should be established and coordinated for the planning and implementation of certain activities proposed and jointly carried out by public institutions for city safety*** [8].

Some of the comprehensive defence activities for city security can be listed as follows: [8]

- Closer defence cooperation between the private and public sectors;
- Civil defence training;
- Psychological defence training;
- Strategic communication; and
- Economic flexibility.

14.3.1 Closer Defence Cooperation Between Private and Public Sectors

It is important to ensure that defence issues are jointly coordinated by public institutions. All departments under the ministries in the city should make sectoral threat assessments and develop plans to address the identified risks. Each unit needs to define threats and mitigation measures in their industry. These units must have threat-response protocols. Collaborations between public institutions, including those responsible for security, the private sector, NGOs, and other stakeholders such as the business community should be formal and visible. NGOs should be given specific roles/duties that will contribute to national defence and their participation in defence planning should be ensured. City managers should proactively collaborate with NGOs and approach each one individually. ***Managers should establish frameworks for self-organising communities, and national and local voluntary networks (networks) ready to help manage a crisis or armed conflict***. The involvement of security units in local events and activities and the civil-military bond between the defence sector and local communities should be strengthened. Annual advocacy training should be provided to selected professional and expert groups, including opinion leaders, public officials, mass media, local authorities, NGOs, and other industries. A few weeks of training will increase awareness of national defence sector processes while focusing on issues such as crisis management, communication, recent defence industry developments, cybersecurity, human security, and other areas. Socially important functions should be defined and given to NGOs to take a more active part in strengthening defence. Managers should partner with NGOs to run public crisis response campaigns and public awareness activities. The community should be educated about providing first aid and how to act in the event of a disaster or

when the first aid warning system is activated.[2] The private sector also plays an important role in city defence. It should be emphasised that the society should operate in a way that contributes to security units in terms of reducing supply security risks related to the goods and services needed by the society, and in promoting peacetime, crisis, and wartime goals [8].

14.3.2 Civil Defence Training

Civil defence is an element of national security. Civil defence is implemented through legal regulations that determine the rights, obligations, and responsibilities of government and local actors, legal and private organisations. More active civil-military coordination, resource sharing, and talent cohesion will lead to closer civil-military relations as part of an effective and strong national defence system. Given the nature of armed conflicts, safe areas should be established close to and easily accessible to these densely populated areas. ***Necessary measures to be taken to ensure that the public infrastructure can be used in the aftermath of a potential emergency or crisis should be determined and training should be provided on this subject.*** Urban dwellers, in particular, should be aware that the responsible authorities may not have the necessary capacity to protect all city dwellers in emergencies or the early stages of armed attacks. Citizens need to be educated about how to care for themselves, family members, and relatives in the early stages of disaster or armed attacks. ***Public institutions should establish frameworks for the response of self-organising communities to the emergency.*** Everyone should know what and how to deal with them as much as they are willing. However, the population needs to be able to organise themselves and to know how to behave in various stages of emergency or armed attack [8].

14.3.3 Psychological Defence Training

The psychological defence of citizens depends on their resilience to negative campaigns and psychological operations against state institutions, processes within the country, or certain events. People's trust in the current way of life, the need for protection and defence should be strengthened. Greater social cohesion increases psychological security as it reduces the likelihood of internal conflicts. Rather than belonging to an (ethnic/religious) group, the community loyal to the state should resist provocation, focus on country/city defence, and avoid ethnic/religious analyses. In times of disaster/emergency/armed attack, various civil society actors such as religious organisations gain great importance in providing people's psychological comfort, giving them strength to endure and overcome difficulties. A permanent dialogue with religious organisations should focus on their roles and actions during a crisis or war. Especially people in emotional and physical distress should be able to continue their religious practices and find comfort in faith [8].

14.3.4 Strategic Communication

Strategic communication at the level of public institutions is used to encourage the population to respond and act in a certain way. In public communication, storytelling and illustrations are used to reveal people's emotional response to a particular subject. Successful implementation of the comprehensive defensive model requires skilled and agile leadership. Information campaigns promoting the Comprehensive Defence model should include opinion leaders explaining why and how the comprehensive defence was built. Public communication and activities should emphasise the past and future continuity of public administration. Here, continuity is ensured by the trust of people in existing processes, participation in public activities, the advancement of culture and history, and the emergence of new traditions. Continuity in public administration relies on public communication during a crisis or when security forces are under threat. In the event of loss of control in management as a result of an external or internal influence, flexible communication between citizens, in particular, will be an assurance of the continuity of public administration. Information flexibility should be reinforced against depictions that will spread through mass media and negatively affect citizens.

[2] Such potential will be one of the partners AFAD and Red Crescent in Turkey. City administrators and Red Crescent and AFAD should meet to provide free first aid training and vital crisis health, survival and recovery instructions to the population of the country.

Professional standards in mass media and important news platforms should be developed to prevent false and unconfirmed information from disseminating and misleading society about events and developments that will affect cities. Public broadcasting services need quality improvement support and improving the quality of public broadcasting helps increase audiences [8].

14.3.5 Economic Flexibility

Economic shocks can cause doubts about citizens' ability to maintain safety and security. Economic resilience should ensure that basic public services continue intact in the event of a disaster or armed attack. Citizens should not worry about their financial and social well-being and future. A responsible approach to city security requires stockpiling of goods needed by citizens living in the city. These goods need to be stocked to ensure that essential utilities are maintained for at least three weeks following the emergency. These essential goods will be distributed to citizens to ensure their stock in case of crisis. Adequate personal reserves must be kept for a person to survive without any assistance for a week. Personal financial security depends on the ability to run businesses despite the crisis or gun attack. Business owners must ensure that their employees are protected from crisis or shooting. Large businesses must ensure that their core operations are not affected by a disaster or armed conflict. These companies must support the economy by providing essential goods and services during an emergency or armed attack. Security units should be responsible for cooperation with large companies that provide supplies, provide necessary information on defence developments, and agree with business owners about what the companies' specific roles and responsibilities will be in defence. Economic flexibility and stability are important to the continuation of the economy despite the crisis or armed conflict. There should be an action plan within the country, based on economic potential and a clear division of responsibility between private and public actors. To ensure overall coordination of economic processes during a crisis or an armed attack, the responsibilities of private sector players should be clearly defined and there should be a responsible authority for this [8].

14.4 CONCLUSION

As a result of the study, the things to be done to carry out comprehensive defence activities for city security are determined as follows:

- Public institutions should be assigned certain duties and roles in city security according to their competence areas;
- Local government bodies (top management of city), NGOs, the business community, public, and other stakeholders should be aware of their role in the city safety system;
- Local-level planning and decision-making frameworks should be implemented to help identify the potential crisis and mitigate its consequences;
- Identify tools and roles vital in providing basic management functions during a hybrid threat, potential crisis, or war;
- City dwellers must respect management, be aware of their responsibilities and be ready to strengthen city security;
- Resist attempts to confuse the minds of city dwellers and explicitly spread disinformation and also have critical thinking; and
- By establishing adequate frameworks and models, the state should ensure that townspeople can self-organise and react when faced with challenges.

14.5 REFERENCES

[1] Adams, R.E., Rohe, W.M., Arcury, T.A. (2005), "Awareness of community-oriented policing and neighborhood perceptions in five small to midsize cities", Journal of Criminal Justice, 33, p. 43-54. doi:10.1016/j.jcrimjus.2004.10.008.

[2] Center on Juvenile and Criminal Justice, (October 1999), "Shattering 'broken windows': An analysis of San Francisco's alternative crime policies". http://www.cjcj.org/uploads/cjcj/documents/shattering.pdf Accessed 09 December 2020.

[3] Clarke, R.V. and Eck, H.E. (2007), Crime Analysis in 60 Small Steps for Problem Solvers", trans. Ahmet Çelik et al., US Department of Justice, Community Based Policing Services, Ankara: Turkish National Police Publication No: 425, 2007.

[4] Durham City and County CPTED Private Sector Task Force, "Crime prevention through environmental design: Durham guide to creating a safer community", Durham County North Carolina. http://www.pac2durham.org/resources/cpted_manual.pdf Accessed 12 December 2020.

[5] Emniyet Genel Müdürlüğü, Toplum Destekli Polislik [General Directorate of Security, Community Policing], https://www.egm.gov.tr/toplum-destekli-polislik# Accessed 10 December 2020).

[6] İbn Haldun (2013). Mukaddime [Preface]. Trans. S. Uludağ. İstanbul: Dergâh Publications.

[7] Kelling, G.L., Wılson, J.Q. (March 1982), "Broken windows: The police and neighborhood safety", The Atlantic, https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/Accessed 10 December 2020.

[8] Republic of Latvia, the Ministry of Defence, Comprehensive National Defence in Latvia, https://www.mod.gov.lv/sites/mod/files/document/Comprehensive%20National%20Defence%20in%20Latvia.docx, Accessed 21 October 2019.

[9] Roepke, W-D., and Thankey, H. (27 February 2019), "Resisting power: The first line of defense", NATO Review, https://www.nato.int/docu/review/2019/Also-in-2019/resilience-the-first-line-of-defence/TR/index.htm, Accessed 22 October 2019.

[10] Thorpe, A. and Gamman, L. (2013), "Walking with Park: Exploring the "reframing" and integration of CPTED principles in neighbourhood regeneration in Seoul, South Korea", Crime Prevention and Community Safety, 15, 3, pp. 207-222.

[11] Türk Dil Kurumu Sözlükleri, [Turkish Language Association Dictionaries, Current Turkish Dictionary], https://sozluk.gov.tr/ Accessed 12 January 2020.

[12] United Nations Centre for Human Settlements (Habitat) (2000), "Safer cities programme, prevention of urban crime", Nairobi, Kenya, Accessed 14 November 2019, https://www.ucl.ac.uk/dpu-projects/drivers_urb_change/urb_society/pdf_violence_rights/HABITAT_Vanderschueren_prevention_urban_crime.pdf

[13] Weber, M. (2012). Şehir: Modern Kentin Oluşumu [The City], Trans. M. Ceylan. İstanbul: Yarın Publications.

Chapter 15 – LEGAL ASPECTS OF INTEGRATING ARMED FORCES INTO INTERNAL SECURITY TASKS: ANALYTICAL CONSTRUCT AND ESTONIAN CASE STUDY

Aleksandr Popov and Leenu Org
Estonian Military Academy
ESTONIA

15.1 ANALYTICAL CONSTRUCT

15.1.1 Introduction

The general theoretical framework for this introduction addresses the issue of the necessity of considering both national and international legal obligations of a state pertaining to its defence. From the point of view of national legislations, every state is free to decide for itself what ought to fall under the purview of the legal system and what can be left to other social devices. Sovereignty grants entities such as states "supreme authority" within and over the territory under their control [2]. From the point of view of law, this establishes a twofold system of governance. States create legally binding rules in order to establish a legal system governing the interaction between the state and its subjects – usually physical persons and legal entities – within the realm of their "sovereignty". Based on the same legal system states have created for the benefit of their internal domain, they provide themselves – as legal subjects created within the framework of a legal system – with the possibility of entering into relations with other states that may or may not (depending on the wishes of the states themselves and the format in which those relations are carried out) bring about legally binding effects.

The interaction between the entities we have come to call "states" is, as one might think, as old as the system of statehood based politics itself. What is pertinent to keep in mind is that just as the legal system within the state creates an expectation of carrying out one's obligation created under the law, so does the international system currently in effect between the states who have decided to adhere to its norms. Unlike the national legal systems, where the will of the state prevails over its subjects – mainly because the state has a law enforcement system in place that guarantees the application of the law to its subjects (well, at least it tries to) – internationally, states are considered to be equal, at least in the eyes of the law. What has been accepted as one of the underlying ideas of the system of interaction in place between the states – some might call it international relations – is the fact that when wrongdoing has occurred, the perpetrator is expected to make amends and bear the penalty for its mistake (Ref. [14], p.21).

From the perspective of international institutions, such idea of sovereignty can be found, in rather more "subtle" formulation, in e.g., Charter of the United Nations, which is kind enough to point our attention at the fact that its sole existence is based upon the "sovereign equality" of its members [26]. No one is technically forced to join the organisation, yet the miracle of international relations has its blessed effect upon the members of international community by making the idea of unified actions targeted towards the achievement of a mutually beneficial end result appealing. This sublime reference to the idea of sovereignty is also connected to the North Atlantic Treaty that already in its preamble pays homage to the "purposes and principles" of the Charter of the United Nations [11].

From the point of view of international legal order, every state is free to decide whether or not it is able and willing to take upon itself obligations that fall outside the scope of its sovereign realm. The key question here is of course the "will" of a state, as a subject of international order, to do or not to do something. For the practical purposes of making an otherwise rather Hobbesian existence of a state more bearable, the solution

to the problem of whether or not there ought to be any will to participate in the international legal order to begin with is, in certain cases (mainly in the setting of constitution-based legal order), connected to the constitutions as the founding document of the state in general and more particularly its legal system as the basis for the "rule of law" governed existence. As it happens, constitutions create the link between the national and international from the point of view of legal validity. When in doubt whether or not to consider certain aspects of international law feasible for the state as a whole, take a look at the constitutional norms and their substance can be of much help.

"Binding" international legal order can't exist without the express "will" of each member of the international community to be bound by that order (Ref. [8], p. 3). Even though, as subjects of legal order, we have grown to be accustomed to the fact that once the law has been proclaimed it has to be obeyed, whether or not one agrees with a particular piece of legislation. Unlike national legal systems, where the concept of "sovereignty" provides the state with a "monopoly of force" that can be used against its subjects in order to force them to follow the "commands" issued by the state via the law, international legal order is based on parity of its members and expects each and every one of them to be open and forthcoming about their willingness to play by the rules established by the sources of international law (Ref. [15], p.471).

For the purposes of this study, the main question is not that much theoretical as it is practical – how many "commands" ought the law issue and where ought they stem from? From the point of view of the classic concept of "sovereignty", every state is "free as a bird" to decide whether or not to do or not to do something. Yet from the point of view of the "political" nature of the international order in place between states since the times of the Peace of Westphalia (or maybe even way before that, depends on how you look at the world), no international legal order can even think about existing without accepting politics as its estranged bedfellow (Ref. [7], p. 9).

15.1.2 National Law as the Basis for the International Obligation

The present text will take the theory of "positivism" as its cornerstone for the analysis of the function of national legislation as the basis of ensuring the functioning of integration of cooperation between national defence forces and internal security forces. In very simple terms, the idea of "positivism" relies on the idea, that laws are merely commands posited by the sovereign authority wielding control over the state [4]. The function of law in such a system is to create two kinds of norms:

1) Norms pertaining to the substance of the legal commands; and
2) Norms creating procedural rules for the evaluation/application of said legal commands.

Following in the footsteps of the idea of "constitutional democracy" that allegedly in its "modern" sense makes law "positive, compulsory and idealistic" (Ref. [5], p. 766) the main statement for the purposes of legal system is as follows: no action prescribed by the law can contradict the norms of the constitution. For the legal prescription pertaining to the either the rights and obligations of the defence forces of the state or powers enshrined in the internal security forces, every action ought to be evaluated based on the legality of the commands contained in the legal framework that creates the baseline for their actions.

In other words, whenever a question pertaining to the legality of specific actions of said forces arises, existence of the legal right to take action is of utmost importance. That is the reason why legislators and administrators who are tasked with creation and application of the laws have to take into account that without proper legal regulation the effectiveness of cooperation and integration of the capabilities of the defence forces and internal security mechanisms is hampered. Proper legal basis serves as a guarantee that ensures the addressees of the command that their actions are within the purview of the legal regulation and therefore they do not have to fear the potential latter legal penalties that are prescribed for those violating the commands of the legal order.

From the point of view of "constitutional democracy" – a political order based on the will of the people to be governed by the laws passed by the sovereign legislative entity elected by the people and for the people – a practical consideration ought to be given to the proper application of the "constitution" as the basis for the existence of not just the legal system but of a state as such. In both cases – defence of the state as such and protection of its internal security – the core values that are seen as worth protecting are the "constitutional order" and "rights" that this order guarantees to the people. Constitution serves as a guarantee for the people that their "voice" will be heard and that the rights they have been granted by the constitution will be uphold. True "democracy" is the "resolved mystery of all constitutions" [9].

The core task of the legislators is to provide for the legal regulation which will make it possible to structure and enlist defence forces tasked with defending the state as an entity of international order. At the same time, the legislators also ought to establish the separate stream of legal regulation which will explain and elaborate upon the different needs of security within the state, and in the purview of the state's legal authority, in order to guarantee the functioning of the state's institutions and provision and protection of the rights of its people.

15.1.3 Role of the Constitution

The Constitution also serves as a nexus between the internal legal regulations of the state and its interaction with other states. The national legal system is the sole creation of the state itself. Yet international interaction between the states has led to the ascent of the new, and to certain extent separate, legal order – "international law". The core difference here is that "international law" can't emerge without the direct will of the states to create a normative framework, separate from the legal norms they have already created in order to establish balance and order within their own sphere of sovereign influence.

In less cryptic language – a national legal system is binding upon everyone who enters the territory of the state. International law can only be considered "binding" upon those members of the international community, who have expressed their explicit "will" to be bound by such norms. Sovereignty gives the state both the right to create the rules within its own realm over which it has governing power and to refuse to be bound by others, to not join the existing normative framework of the international law.

If for constitutional democracies it is the "constitution" that serves as the cornerstone of the legal system, then for the practical purposes of international legal order it is the treaties concluded between the states that create the "normativity" to which the states have bowed their crowns. Every state can make a choice – either to bind itself or not to bind itself with the existing framework. Interestingly, they don't have to accept all the treaties that exist out there, they can pick and choose among the existing norms, just like one would at a well-stocked buffet table. Sadly, for those of us ending up at the mercy of the national legal systems, such opportunities are rarely possible.

International legal order functions on the premise of "independent choice" – states can make a decision, whether or not they want to take upon themselves any obligations. Of course the political reality of such choice is that such "choices" are rarely made in a vacuum. In the case of attempting to ensure the security of the state, both external and internal, the choices will be dictated not merely by the ability to taken on rights and obligations but also by the political reality – it is far more easy to attempt securing one's interest when you have allies.

15.2 ESTONIAN CASE STUDY

15.2.1 Introduction

The purpose of this case study is to describe how the Estonian Defence Forces (EDF) and Estonian Defence League (EDL) are integrated into Internal Security Tasks. More specifically, it focuses on legislation, the tasks,

use of force, training requirements and command and control. The Estonian Defence Forces comprises of professional military personnel, conscripts, and reservists. The Estonian Defence League is a voluntary national defence organisation operating in the area of government of the Estonian Ministry of Defence, which is organised in accordance with military principles, possesses weapons and holds exercises of a military nature [3].

15.2.2 Threat Perception

According to National Security Concept of Estonia (NSCE) immediate threats to Estonia's security primarily depend on the security situation in the Euro-Atlantic region and the relations between its neighbouring countries (Ref. [10], p 4). NSCE points out that asymmetric threats that know no state borders and whose sources are difficult to detect have emerged and their impact on security is comparable to traditional security threats [10]. Today it is increasingly clear that security is influenced by economic instability; developments in the cyberspace; technology-related threats; radicalisation and terrorism; organised crime and corruption; migration flows; and a variety of other emergencies [10]. Those threats have become more real and serious due to Russia's aggression towards Ukraine. Since Russia is a neighbouring country to Estonia and by so, a neighbouring country to EU and NATO as well. Therefore, Estonia does not only have an obligation to its citizens to provide security, but it also needs to maintain the security for EU and NATO.

Estonia's security policy is based on a broad security concept. The broad security concept foresees increased and deepened integration of and cooperation between the state institutions, but also at an international level, and the involvement of all sectors of society [10]. The broad security concept includes a comprehensive national defence concept, which comprises 5 main lines of activity: military defence, national security, sustainability of a state and society, strategic communication, and international activities (Ref. [16], p.9). The Estonian National Defence Development Plan 2022 – 2031 (ENDDP) states that the Armed Forces also have a role in ensuring the internal security of Estonia [16]. Even though the primary function of the EDF is military defence of the state and participation in collective self-defence, the EDF and EDL are working closely together with other institutions.

15.2.3 Overview of Estonian Legislation

There are no international regulations concerning how states can use their armed forces within in their territory. States evaluate the need to integrate armed forces into internal security tasks based on their requirements concerning the level of threat and the overall security situation. The Constitution of the Republic of Estonia dedicates an entire chapter to National Defence [17]. This chapter regulates the general aspects of National Defence – different levels of state of emergency; obligations of citizens; restricting of fundamental rights, freedoms, and duties; requirements of necessary laws, etc. However, it does not regulate the integration of armed forces into internal security tasks per se. The Supreme Court of Estonia has said that the state must evaluate security threats according to current events [6]. Comments to the Constitution complement this statement further by saying that nowadays threats affect a state both externally and internally [1]. Furthermore, functions of state institutions must take into account what would be the most efficient way of using state resources the most effectively. Estonia is a small country with limited resources. According to Statistics Estonia the population of Estonia in 2022 was only 1,331 796 million people. Thus, Estonia needs to use its resources efficiently and this applies to providing security in Estonia. This means that the functions of armed forces are not only limited to providing military defence, however, armed forces can also contribute to assisting in maintaining public order and internal security as long as the functions of armed forces are defined clearly and enforced by effective civil control measures [1].

Even though the Estonian Constitution does not provide direct wording of using armed forces for the purpose of providing security and ensuring public order, it is, however, in accordance with the principles of the Constitution. Moreover, the Constitution provides which laws and regulations must be in force. Laws concerning National Defence are mentioned in the Constitution and those laws, enforced by the Parliament, include norms about the above-mentioned clearly defined functions of the armed forces and civil control procedures.

Laws that include regulations concerning integrating armed forces to internal security tasks are the following:

1) **The Estonian Defence Forces Act [19] –** includes the tasks of EDF, use of force and the list of equipment allowed for the members of the EDF.
2) **The Estonian Defence League Act [12] –** includes the tasks of EDL, use of force and the list of equipment allowed for the members of the EDL.
3) **Law Enforcement Act [20] –** regulates principles and organisation or law enforcement, direct coercion, and special measures. Also includes procedures for integrating EDF/EDL into law enforcement tasks.
4) **State of Emergency Act [25] –** regulates principles and procedures for situations where there is a threat against Estonian constitutional order. Also includes procedures for integrating EDF/EDL into law enforcement tasks.
5) **Emergency Act [18] –** regulates crisis management procedures and obligations of institutions. Also includes procedures for integrating EDF/EDL into law enforcement tasks.
6) **Rescue Act [23] –** regulates principles, tasks and procedures for the Rescue Board and rescue events. Also includes procedures for requiring the assistance of EDF/EDL in cases of rescue events.
7) **Police and Border Guard Act [22] –** This Act provides for the functions, rights and organisation of the police and the legal bases for police service. It includes police tasks that the EDF/EDL can perform if integrated into law enforcement tasks.
8) **Penal Code [21] –** regulates the imposition of punishments. It also includes the list of crimes that EDF/EDL can be used in order to prevent those crimes if integrated into law enforcement tasks.
9) **State Borders Act [24] –** regulates Estonian State Border related aspects, as well as tasks that the EDF/EDL can perform if integrated into law enforcement tasks.

Laws refer to subsequent governmental and ministerial regulations that provide more details and, also procedures for involving the EDF and the EDL. Acts listed above also cross reference each other.

The EDF Act and EDL Act both list the tasks that those organisations can fulfil in order to participate in ensuring public safety and security. The rest of the Acts listed above include more details concerning the scope of the said act, e.g., Rescue Act regulates procedures concerning EDF and EDL in case of a rescue event, etc. Police and Border Guard Act, Penal Code and State Borders Act do not include any regulations concerning integrating armed forces into internal security tasks. However, those Acts regulate certain aspects that are connected to the tasks of EDF and EDL. e.g., The Law Enforcement Act says that EDF and EDL can be used to assist police in order to prevent certain types of crimes; the list of those crimes is regulated in Penal Code. This type of cross-referencing is very common and there exists a lot of it concerning this topic and the above-mentioned laws.

15.2.4 Tasks of the EDF and the EDL

Like other countries, the use of armed forces within Estonian territory is limited. Belgium defines five areas in which armed forces may be used: rescue operations; medical, sanitary, and psychosocial assistance; emergency site policing and support to police force; logistical support and information [12] (Belgian Case Study). The tasks of the Norwegian Armed Forces concerning assistance to the Police are (in a simplified version) limited to prevention of harmful attacks, search and seizure of dangerous persons, and rescue situations [12] (Norwegian Case Study). The tasks with which that armed forces in Estonia can assist other institutions are quite similar in nature – maintaining public order, rescue situations, prevention of crimes, etc.

Both the EDF and the EDL can participate in ensuring public order and security in Estonia. The tasks of the EDF are regulated in the EDF Act and the tasks of the EDL are regulated in the EDL Act. Those tasks are not connected to military defence of the state and participation in collective self-defence.

The wording in the Acts concerning the tasks is somewhat different, however, the content of the norms is almost identical. Except for the EDL task concerning cyber security. The EDF does not perform that task in connection with assisting other institutions. In the EDF Act the tasks are divided by whether or not it is allowed to use force for the completion of the tasks. In the EDL Act the tasks are listed without any classification of the content. Tasks are depicted in Appendix 15-1.

The preconditions for involving armed forces in internal security tasks are that the institution has exhausted its own resources and, thus, is not able to fulfil their duties. In addition, it is required that personnel who are assigned to assist another institution, have the required training for the specific task (e.g., if they are used to put out a fire, they must be trained for that). The institution that requests the help from either the EDF or the EDL, must also reimburse for the expenses.

In case other institutions require assistance from the armed forces, they most likely first submit a request to the EDL and not the EDF. Even though both organisations work closely together with other institutions (Police and Border Guard, Rescue Board, Estonian Internal Security Service, etc), it is still the EDL that is more integrated into the work of other institutions. e.g., the EDL conducts more exercises together with the Police and Border Guard. The EDF units/personnel/equipment would be requested in case of either a more serious crisis or a more specific task.

For example, a cargo plane landed on Ülemiste Lake ice in 2010 during winter time. Ülemiste Lake is situated at the end of the airport runway and the plane conducted an emergency landing. Assets of the EDF logistical units were used to extract the plane from ice. Another example is the deployment of the EDF field hospital in 2020 in Kuressaare in order to provide assistance in the fight with COVID-19. The EDL units were integrated with the Police and Border Guard during the fight with COVID-19 in 2020 in order to assist the police to maintain public order on the streets in certain locations of Estonia. Amongst other things, their task was to make sure people were following restrictions provided by the Government and maintain the 2+2 rule.

15.2.5 Procedures

Procedures for integrating armed forces into internal security tasks are regulated in four different Acts (Emergency Act, State of Emergency Act, Law Enforcement Act and Regulation of Estonia Government No 144 concerning the rules for involving The Estonian Defence Forces and the Defence League in the performance of police tasks, in the solution of rescue events and emergency). Even though the procedures are regulated in different Acts, they are, nevertheless, very similar. Procedures include level of authority requirements, use of force and requirements for the content of the decision (description of the task, time limit, no of personnel, deadline, limits for the territory, etc.).

The level of authority for making a decision on involving armed forces depends on the type of the assignment. Tasks involving use of force (direct coercion) have three-layer system. Firstly, an appropriate minister must request tasks involving use of force. Secondly, the Minister of Defence approves using armed forces. Thirdly, the Estonian Government authorises with its decree tasks that include use of force and Estonian President must approve this decree.

Authorisation procedures are easier for assignments in which the use of force is not allowed. A request for involving armed forces is made by the institution requiring assistance. Commanders of the EDF and the EDL or unit commanders authorise tasks that have to be performed without the use of force. Thus, it is solved on working level and no political level is included in those cases.

Common to all the tasks is that the units or personnel of the EDF/EDL are placed under the command of the official of the institution. This means the EDF/EDL are fulfilling the obligations of the said institution.

15.2.6 Authorities

15.2.6.1 Command Authority

As stated in the previous paragraph, units or personnel of the EDF/EDL are placed under the command of the official of an institution that is requesting the assistance of the armed forces. Whilst the armed forces are used to operating with NATO degrees of authority (FULLCOM, OPCOM, OPCON, TACOM and TACON), those classifications of authority are not used by civilian institutions. NATO degrees of authority include aspects of task organisation, assigning missions, assigning tasks, delegation of command authority, coordinating movements, planning and coordination and administrative/logistic responsibility [12]. In order to better comprehend how command authority functions in cases of integrating armed forces into internal security tasks it is important to analyse each aspect separately.

One of the most important aspects about the degree of command authority is whether civilian institution can task organise the assigned element. Practice has shown this aspect depends on the mission. There are cases where commanders have given their instructions concerning this aspect. For example, some commanders have given instructions that a platoon can only be divided into squads. Then C2 is preserved by squad leader and radio communication capability. However, in some cases units have been divided into 2-person teams. The latter was the case where the EDL helped Police and Border Guard patrol state border during COVID-19 restrictions in 2020. Therefore, task organisations depend on the mission, capabilities of the unit and the intent of the commander.

Another important aspect is whether missions and/or tasks can be assigned to the unit/personnel. Mission assigned to the units/personnel of the EDF/EDL is stated either in the governmental decree (in case the tasks include the use of direct coercion) or stated in the request issued by the institution and approved by either EDF/EDL commander or a unit commander (in cases where direct coercion is not used). Thus, mission is already assigned to the unit/personnel of the EDF/EDL. Authority to assign tasks is essential and the official of civilian institution should be able to assign tasks as long as they are in accordance with the mission.

Further delegating command authority is another aspect that is essential. Even though units/personnel of the EDF/EDL are placed under the command of one official, usually this official is high ranking official who may not be operating on the field himself/herself. Normally, when armed forces are assisting Police and Border Guard, the units are placed under the command of regional prefect. However, those units/personnel are working in the field together with police patrols or other types of smaller units. Therefore, those patrols should have the authority to assign tasks in their capacity as well. Currently this is not specifically regulated in either relevant Acts or subsequent Governmental regulations.

It is also essential that civilian institutions have the authority to conduct the coordination of other aspects, such as movements, force protection and planning, and coordination. These are normal functions necessary to ensure good cooperation between organisations and units. Mostly these aspects are dealt with on a working level, rather than being regulated specifically.

While administrative and logistic responsibility lies only with FULLCOM within the NATO context, the situation is different when assisting civilian institutions. Firstly, it is the responsibility of civilian institutions to request the assistance and to follow through with the correct procedures. Secondly, civilian institutions are required to reimburse for the costs of the assistance. Thirdly, in case of using direct coercion, civilian institutions are required to provide either Rules of Engagement or Code of Conduct because essentially the EDF/EDL units/personnel are fulfilling the tasks of those institutions and it should be done according to their rules and procedures.

Therefore, it is not possible to make a parallel with NATO degrees of authority because they do not apply the same way as they would within military cooperation. Furthermore, civilian authorities are not familiar with

NATO command authority. Therefore, there is no point in assigning units to them with, for example, OPCOM, because they do not understand what this means. In order to establish good cooperation with civilian institutions, it is still relevant for the commander to give them list of caveats or description of limits that depend on capabilities of the units/personnel. Those caveats can follow the logic of those essential aspects of NATO degrees of authority (task organisation, assigning missions/tasks, etc).

15.2.6.2 Special Measures

Special measures are activities that law enforcement institutions can implement in order to prevent, stop, and eliminate a violation. Special measures normally include limiting a person's fundamental rights and freedoms. The Law Enforcement Act regulates the specifics of special measures. Special measures can be used by the EDF/EDL for tasks No 1-3 depicted in Appendix 15-1. All those tasks also include using direct coercion.

EDF/EDL can implement special measures in cases requested by either the Rescue Board or the Police and Border Guard. Special measures that the EDF/EDL can use are the following: injunction and application of administrative coercion, questioning and requesting documents, identification of a person, checking and detecting alcohol intoxication on the spot, detection of the use of a narcotic or psychotropic substance or other intoxicating substance or intoxication caused by it, delivering an intoxicated person to sober up, restraining order, stopping a vehicle, detention of a person, security check, examination of a person, examination of movable property, entry into premises, examination of premises, storing of movable property.

It is required that the EDF/EDL units integrated with civilian institutions obtain the necessary training required for the specific task. Some units have specific training connected to the unit's specialty (e.g., Military Police). However, very often, this training is merely ad hoc Rules of Engagement training on site. Regulations do not specify the type of training required and it can be decided by the EDF/EDL whether units have the necessary training. Since the use of special measures is relatively new (since 2020) and since special measures very often means restricting a person's fundamental freedoms and rights, it is important that those measures are used correctly by the members of the EDF/EDL.

15.2.7 Use of Force

The type of use of force used by armed forces in assisting other institutions in Estonian territory is direct coercion. Direct coercion is allowed only with three tasks (See Appendix 15-1). Direct coercion is regulated in the Law Enforcement Act, and it is used in law enforcement tasks. Direct coercion shall mean affecting of a natural person (hereinafter person), an animal or a thing by physical force, special equipment, or a weapon [13]. Before the application of direct coercion, a law enforcement agency shall be required to caution the person with regard to whom or with regard to an animal or thing in the person's ownership or possession the law enforcement agency is planning to apply direct coercion [13]. Direct coercion is escalating use of force where use of deadly force should always be the last resort and be only allowed in extreme cases.

Direct coercion is a different type of use of force for the armed forces. Normally armed forces train and use force in accordance with the Law of Armed Conflict (LOAC). Using force in accordance with LOAC sets very different standards, e.g., a soldier can use deadly force against an enemy combatant upon positive identification. Meaning that the enemy can be engaged automatically, and it does not matter whether the combatant is firing at you, or he/she is loading a truck. Direct coercion is much more restrictive and especially for members of the armed forces who are trained to use force differently. Thus, this can create many problems with excessive use of force. Moreover, the force is being used against a state's own citizens. Therefore, proper training in direct coercion is extremely important whilst working together with civilian institutions, e.g., the police.

The training of armed forces in direct coercion is not systematic. The police train some EDL units regularly. However, if the EDF units are used to assist other institutions with the right to use direct coercion, then usually the police provide those units necessary training on the spot. Some EDF units get regular training in direct coercion (e.g., military police). In addition, force protection units get minimal training in direct coercion and officers learn about direct coercion in Estonian Military Academy. However, the overall level of training is not sufficient.

There is also a difference between equipment and weapons used by the police and the EDF/EDL (Table 15-1). As previously mentioned, the use of force with direct coercion must have escalating measures. Since the list of weapons and special equipment is much shorter with the EDF/EDL compared to the police, it can create situations where member of the EDF/EDL will most likely use excessive force due to the lack of "softer"equipment.

Table 15-1: Special Equipment and Weapons Used for Direct Coercion.

Police Weapons and Special Equipment	EDF End EDL Weapons and Special Equipment
Weapons: 1) A firearm; 2) A gas weapon; 3) A pneumatic weapon; 4) A cut-and-thrust weapon; and 5) An electric shock weapon. Other special equipment: 1) Handcuffs; 2) Shackles; 3) Binding means; 4) A restraint jacket or a restraint chair; 5) A service animal; 6) A technical barrier; 7) A means to force a vehicle to stop; 8) A water cannon; 9) Grenades evoking tears, or smoke, sonic, light, or other effect, or a sensation of pain; 10) An explosive device for special purposes which is not used against a person; 11) A lighting and audio device for special purposes; and 12) A colouring and marking device for special purposes	Weapons: 1) A firearm; 2) A gas weapon; and 3) A cut-and-thrust weapon. Other special equipment: 1) Handcuffs; 2) Binding means; 3) A service animal; and 4) A restraint jacket (only EDF).

15.2.8 Summary and Conclusions

Since the main task of armed forces is to provide military defence of the state, armed forces are not meant to be used for law enforcement functions. Integrating armed forces into internal security tasks must be in accordance with the Constitution of the state and laws must clearly define those tasks.

In Estonia, those requirements are fulfilled. However, all the aspects of this topic are regulated in 9 different Acts and there is also lot of cross-referencing among those Acts. Therefore, the legal basis for integrating armed forces into internal security tasks is very difficult to follow.

Armed forces can provide assistance to other institutions (most commonly Police and Border Guard, Rescue Board) in case those institutions are not able to fulfil their duties, or they lack necessary capabilities. Those tasks are connected to crisis events that endanger people's lives or events that are estimated to cause a lot of financial damage. Some of the tasks include using direct coercion. Those tasks are authorised by the Estonian Government with its decree, which must be approved by the Estonian President. Tasks without the authority to use direct coercion can be approved by commanders of the EDF/EDL.

Units/personnel of the EDF/EDL are placed under the command of an official of the institutions that have requested the assistance. Since the main responsibility of the EDF is to ensure the military defence of Estonia, the EDL units are commonly used more often. So far, the EDF units/personnel that have assisted other institutions have been in connection with a specific task or capability (e.g., logistical, or medical capability). However, when institutions require manpower, they most likely will turn to the EDL first.

15.3 REFERENCES

[1] Annotated Edition of the Constitution of the Republic of Estonia, paragraph 8. Available at: https://pohiseadus.ee/sisu/3603 Accessed 22 Aug 2022.

[2] Besson, A. (last updated April 2011), "Sovereignty" in A. Peters and R. Wolfrum (Eds), The Max Planck Encyclopedia of Public International Law, Oxford University Press, www.mpepil.com Accessed 26 May 2022.

[3] Estonian Defence League, available at: https://www.kaitseliit.ee/en/edl Accessed 22 Aug 2022.

[4] Green, L., and Adams, T. "Legal Positivism", (2019), The Stanford Encyclopedia of Philosophy, Winter 2019 edition, https://plato.stanford.edu/entries/legal-positivism/ Retrieved 26 May 2022.

[5] Habermas, J. (2001), Constitutional democracy: A paradoxical union of contradictory principles?", Political Theory 29(6).

[6] Judgement of 19 December 2019, Defence Forces Organisation Act, 5-19-38/15, RKPJKo 19.12.2019, 5-19-38/15, paragraph 91.

[7] Koskenniemi, M. (1990), "The Politics of International Law", European Journal of International Law, 1(1).

[8] Lauterpacht, H. (2011), The Function of Law in the International Community, Oxford University Press.

[9] Marx, K. "Critique of Hegel's philosophy of right", https://www.marxists.org/archive/marx/works/1843/critique-hpr/ch02.htm Retrieved 26 May 2022.

[10] National Security Concept of Estonia, 2017. Available at: https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_security_concept_2017.pdf

[11] NATO (1949), Preamble, The North Atlantic Treaty, https://www.nato.int/cps/en/natolive/official_texts_17120.htm Accessed 22 Aug 2022.

[12] NATO STO, "Conceptual framework for comprehensive national defence system", Interim report of the SAS-152 study: Review of literature, case studies and preliminary findings. NATO STO Technical Report STO-TR-SAS-152-Part-I. Pre-release. ISBN 978-92-837-2330-1. DOI: 10.14339/STO-TR-SAS-152-Part-I.

[13] North Atlantic Treaty Organization (NATO) (2019), AJP-3. Allied Joint Publication. Edition C version 1. February 2019. Allied Joint Doctrine for the Conduct of Operations, pp. 1-40.

[14] Permanent Court of International Justice (1927), Case Concerning the Factory at Chorzow (Claim for Indemnity) (Jurisdiction, Germany v. Poland, Judgment, PCIJ Series A, Judgment, No. 9, 4.

[15] Postema, G.J. (2001), "Law as command: The model of command in modern jurisprudence", Philosophical Issues 11, pp. 470-501.

[16] Republic of Estonia Government Office, Estonian National Defence Development Plan 2012 – 2031, Available at: https://riigikantselei.ee/el-poliitika-julgeolek-ja-riigikaitse/julgeoleku-ja-riigikaitse-koordineerimine Accessed 22 Aug 2022.

[17] Riigi Teataja (1992), Constitution of the Republic of Estonia, Chapter X, available at: https://www.riigiteataja.ee/en/eli/530122020003/consolide

[18] Riigi Teataja, Emergency Act, English version available at: https://www.riigiteataja.ee/en/eli/528062021002/consolide Accessed 22 Aug 2022.

[19] Riigi Teataja, Estonian Defence Forces Organisation Act, English version available at: https://www.riigiteataja.ee/en/eli/512062020001/consolide Accessed 22 Aug 2022.

[20] Riigi Teataja, Law Enforcement Act, English version available at: https://www.riigiteataja.ee/en/eli/503032021004/consolide Accessed 22 Aug 2022.

[21] Riigi Teataja, Penal Code, English version available at: https://www.riigiteataja.ee/en/eli/510052022003/consolide Accessed 22 Aug 2022.

[22] Riigi Teataja, Police and Border Guard Act, English version available at: https://www.riigiteataja.ee/en/eli/510082021002/consolide Accessed 22 Aug 2022.

[23] Riigi Teataja, Rescue Act, English version available at: https://www.riigiteataja.ee/en/eli/512022021001/consolide Accessed 22 Aug 2022.

[24] Riigi Teataja, State Borders Act, English version available at: https://www.riigiteataja.ee/en/eli/507072021001/consolide Accessed 22 Aug 2022.

[25] Riigi Teataja, State of Emergency Act, English version available at: https://www.riigiteataja.ee/en/eli/512052020002/consolide Accessed 22 Aug 2022.

[26] Riigi Teataja, The Estonian Defence League Act, English version available at: https://www.riigiteataja.ee/en/eli/513042022002/consolide Accessed 22 Aug 2022.

[27] United Nations Charter (1945), Chapter 1, Purposes and Principles, Article 2(1). 24 Oct 1945, 1 UNTS XVI.

Appendix 15-1: TASKS OF THE EDF/EDL AND LEVEL OF AUTHORITIES

No	Task	EDF	EDL	Request Made By	Approved By	Use of Direct Coercion
1.	Prevention and obstruction of an attack against national defence objects, of an illegal crossing of the state border or a temporary control line and of criminal offences pursuant to the procedure provided for in the Law Enforcement Act.	+	+	Minister responsible for public order coordinated with Minister of Defence	Government with the consent of the President	+
2.	The solution of emergency situation pursuant to the procedure provided for in the State of Emergency Act.	+	+	Minister responsible for homeland security coordinated with Minister of Defence	Government with the consent of the President	+
3.	The regulation of traffic and ensuring of safety in an emergency situation area pursuant to the procedure provided for in the Emergency Act.	+	+	Minister responsible for crisis management coordinated with Minister of Defence	Government with the consent of the President	+
4.	The performance of emergency situation work pursuant to the procedure provided for in the Emergency Act.	+	+	Person in charge of emergency situation work	COM EDF/EDL or unit COM authorised by them	
5.	The solution of a rescue event pursuant to the procedure provided for in the Rescue Act.	+	+	Estonian Rescue Board	COM EDF/EDL or unit COM authorised by them	
6.	The performance of the police duties provided for in clauses 3 (1) 1), 4), 6), and 8) of the Police and Border Guard Act and subsection 16 (3) of the Emergency Act.	+	+	Police and Border Guard	COM EDF/EDL or unit COM authorised by them	
7.	Ensuring cyber security under the direction of a competent authority.		+		COM EDL	

Chapter 16 – CONCEPT MODEL OF COMBINED HEADQUARTERS

Jaan Murumets and Aarne Ermus
Estonian Military Academy
ESTONIA

16.1 INTRODUCTION

One aim of the Phase I case studies was to identify recurring themes and common shortfalls in implementing the comprehensive defence concept [12]. The small number of participating nations inevitably limits the scope and depth of topics that conceivably could be addressed in this study. The fact that different nations are at the different stages in implementing the comprehensive approach from accepting the philosophical idea of comprehensive approach [12] (Latvian case study) to enhancing already existing total defence systems [12] (Norwegian case study) also shapes the bounds of the possible. By describing the Comprehensive Defence Systems of five different nations, case studies helped to identify common challenges and shortfalls. The aim of this chapter is to discuss and propose a solution to enhance the command and control systems of the comprehensive defence. The proposed model does not take into account the differences and limits of national legal frameworks.

Based on observations from Phase I studies, one could argue that comprehensive defence systems can, in a generic way, be described as complex endeavours consisting of a large number of diverse actors with often conflicting objectives and perceptions operating under ambiguous command lines which creates challenges in implementing the common tasks [12].

The case studies have identified few areas of concern and drawn few conclusions. First, the availability of resources may set limits for the single-agency actions in the comprehensive defence:

> *...CA is the only solution to the fact that no actor, organisation or even country has sufficient means at its disposal to effectively navigate a major or complex crisis (as is continuously being demonstrated by the COVID-19 crisis). Thereby, collaboration between stakeholders with underlying C2 mechanisms, joint financing mechanisms, joint plans, and joint strategies are indispensable (Belgian case study)* [12].

Second, lack of unity and mutual understanding among different actors will impede timely planning and execution of comprehensive defence tasks. Planning for, and conduct of, operations in a complex, multi-domain environment with involvement of different military, paramilitary and non-military organisations, to include countering hybrid threats, requires a coherent conceptual framework to ensure shared understanding of missions, tasks, capability requirements and concepts of operations [12].

Third, the dynamics and complexity of modern crises requires a flexible and agile crisis management system, which can only be built on common situational awareness and close cooperation between the main actors of comprehensive defence.

Fourth, the main warfighting principles [15] – unity of effort, concentration of force, economy of effort, freedom of actions, definition of objectives, flexibility, initiative, offensive spirit, surprise, simplicity and maintenance of morale – can be and should be taken into account in comprehensive defence.

One possible solution to address these challenges whilst meeting the systemic requirements can be the network of combined Comprehensive Defence Headquarters (CDHQ), working as command, control, and decision support body for crisis managers, as well as coordination and de-confliction framework in the

context of preparatory work. Such a set of state, regional and site level headquarters would require permanent infrastructure and dedicated and trained personnel, retain limited operational capability round the clock, and be gradually expanded as needed. Using unified procedures, operational language, communication means and shared situational awareness in addition to the common training will ensure the preparedness to act and timely respond to unwanted events. This solution would also preserve the strengths of the traditional system: agency-based capability development and knowledge management, be it firefighting, protection of public order, or ambulance services.

16.2 SUPPORTING CONCEPTS

When thinking about the concept of comprehensive defence, it is important to realise that while the operational architecture of a modern Western military organisation – who does what, when, where, together with whom using what Task Organisation and equipment, applying what Command and Control arrangements, and following what doctrine – is well established and documented; Missions and Tasks for **non-defence** agencies appear to exist mainly in political language only. In other words, a coherent and comprehensive framework of standardised activities – descriptors, tactics, techniques, procedures, Measures of Effectiveness – does not exist outside of the Defence Forces. For the purpose of this study, the national comprehensive defence system is broadly understood as a **coordinated cooperation of different government, public, private, and non-governmental organisations with military structures, integrating different operating concepts, methods of Command and Control, information flows, and processes and procedures** (Ref. [11], p. 3). During the working group deliberations, it became clear that a uniform approach is required to describe, and ultimately – compare the elements of, the diverse universe of concepts, actors and standard operating procedures across multiple countries and different institutional frameworks. Two main supporting concepts were agreed to be applicable: concept of escalation to underpin the institutional dynamic of authorities and actions, particularly within the context of crisis management effort; and a generic framework of levels of decision making that would enable to group and organise activities of military and non-military actors in a comprehensive manner.

Furthermore, three additional concepts were used to develop the framework for the combined headquarters. The concept of command and control agility [17] was used to address the flexibility and speed of coping with uncertainties and complexity of possible crises. The concept of crisis management phases [6] was used to address the volatility and unpredictability of the crises and to offer a holistic framework to address the whole continuum of events from pre-crisis to post-crisis status quo. Finally, the concept of stakeholders was used to address the diversity and complexity of actors in the comprehensive defence system.

16.2.1 Concept of Escalation

In order to properly understand and discuss roles and functions, authorities and competencies of various actors within the concept of comprehensive defence, one needs a framework that helps to focus on the most important question: ‘Who does what?’ Which agency has the lead in writing the plan? Which agency coordinates the plan? Which agency is responsible to execute the plan? Which agency has the resources to implement the plan? It is of key importance to dissimilate various roles and missions of all government agencies and voluntary organisations that participate in the defence of the country; “integrate” the efforts performed by non-defence organisations with those of the Armed Forces; address the issues of the “transfer of authority” in crisis and transition to war; and finally, determine who establishes training standards and logistic priorities [4]. The construct that enables to understand the institutional dynamic of crisis management is that of four-tier concept of escalation.

In a nutshell, the four tiers can be described as follows:

- **Peacetime:** regular activities are carried by the peacetime defence and other structures, at a regular pace to ensure readiness and the maintenance of capabilities.
- **Tension:** the activities of the peacetime structures are intensified. The pace of activities is raised and capabilities to gather and disseminate information are enhanced.
- **Crisis:** A state of higher readiness is declared. Key facilities are provided with additional security measures, the reserves are activated selectively or partially, and inter-agency coordination is strengthened.
- **Wartime:** the application of all national resources for wartime needs [4].

Activities at each tier are carried out under increasing operations tempo and changing legal and command and control arrangements.

Tier One. Peacetime: Routine activities on day-to-day schedule

Encompasses routine activities using peacetime institutional arrangements. Inter-agency relationships remain routine.

Tier Two. Tension: Increased activities within the peacetime structure

Encompasses increased operational tempo, increased surveillance, and increased intelligence gathering and dissemination. Domestic and international inter-ministry cooperation increases without change in institutional relationships. The typical activities within this tier would include increase in activities of Ministries and agencies, and changes in Standard Operating Procedures (SOPs) as authorised by the President or Cabinet of Ministers; activation of relevant Crisis Management Centre (CMC), and deployment of local CMCs as required, depending upon the nature of situation; increase in diplomatic activity; and select cancellation of leave and holidays.

Tier Three. Crisis: Emergency situation, unsolvable within peacetime institutional and procedural arrangements, which may include partial activation of reserve assets

Encompasses increased inter-agency coordination and transition of leadership to a Ministry or agency in charge, depending upon the nature of the crisis. The typical activities within this tier would include bringing elements of the Armed Forces to the required state of readiness and partial activation of reserves, if required; increased diplomatic efforts; activation of specific legal arrangements (mechanisms); changes in peacetime institutional arrangements, SOPs, and reallocation of existing assets as needed; and coordination and control of activities of designated capabilities to mitigate the crisis.

Tier Four. Wartime: Utilisation of all national resources to defend national sovereignty

The typical activities within this tier would include declaration of a state of war by Parliament; implementation of legal acts related to the state of war; and full or partial mobilisation of defence assets, to include transition of designated assets from other Ministries under the command of the Chief of Defence (Ref. [9], p. 233).

As one could notice from the above, there is no established formal set of indicators that would trigger the tier change. Quite the contrary, it is evident that the next tier can be considered if and when the activity pattern at lower tier is perceived to become inadequate. Therefore, the decision to take the system from one tier to another is always subjective and political in nature. As seen from Phase I case studies, the roles and responsibilities of participating agencies tend to change in the process of escalation. The degree of such changes depends on legal arrangements of the particular country.

16.2.2 Levels of Decision Making

Another important construct that provides for clarity and consistency in the concept of comprehensive defence is that of levels of decision making, corresponding to respective levels of war in military thinking. In the Western military community, three levels of war – strategic, operational, and tactical – are commonly accepted. Each of the corresponding command levels has its own scope and specific problems to deal with. As defined within the NATO community, levels of war encompass the following activities:

1) **Strategic Level.** The level of war at which a nation or group of nations determines national or multinational security objectives and deploys national, including military, resources to achieve them.
2) **Operational Level.** The level of war at which campaigns and major operations are planned, conducted and sustained to accomplish strategic objectives within theatres of operation.
3) **Tactical Level.** The level at which activities, battles and engagements are planned and executed to accomplish military objectives assigned to tactical formations and units [15].

For the sake of clarity and consistency in comprehensive defence concept, hence, it is crucial to recognise to which level of decision making, and with what particular authority, existing command and control structures, including top civilian leaders belong. Even more important is the issue of levels of decision making for comprehensive defence organisations in transition, when division lines between authority and responsibility of different agencies tend to distort (Ref. [9], p. 150). It is clear that some concept of levels of decision is also used in organisations and agencies outside the defence domain. However, approaches to defining the levels and dividing decision-making authority inside the organisation differs from agency to agency [11]. Such inconsistency creates additional friction for the comprehensive defence system.

Therefore, for the purposes of adapting the existing military doctrinal body to be used within the concept of comprehensive defence, the three levels of decision making can be established: site, region and state (nation). This system copies, in a generic way, the most commonly used division of decision levels in civilian agencies (Estonian Case study) [11]:

> **Level 1: Site.** This level is similar to a tactical level of war. Site is defined as the geographical location, where the emergency or other event occurs and/or damage has been done. At this level, the activities to resolve the situation are executed. Typically, such activities are combined undertakings of different agencies. Typical coordinating activities on this level are related to assigning tasks to the units, and clarifying the roles and responsibilities. To ensure the unity and economy of effort, the lead agency representative should have decision-making authorities similar to Tactical Control (TACON) in the military [14].
>
> **Level 2: Region.** This level is similar to the operational level of war. Unlike the classical military interpretation of operational level, regional level in comprehensive defence concept is primarily tasked with coordinating and sustaining the simultaneous crisis-resolution efforts of multiple agencies on multiple sites or on larger geographic area than single site. On this level, the main focus is not on the real-time crisis resolution actions, but allocation of recourses to support the continuity of actions.
>
> **Level 3: State (Nation).** This level in comprehensive defence concept corresponds to a strategic level of war. As the military analogue, this level focuses on establishing the policies and priorities and determining the objectives. Here the unity of effort of the political level and responding agencies' level is ensured.

16.2.3 Command and Control (C2) Agility

Comprehensive national defence requires orchestrated effort of different stakeholders to achieve the desired results in solving complex problems in uncertain and volatile environment. Volatility and unpredictability of

situations requires from the command system high flexibility and adaptability. A significant number of different actors with varying problem-solving practices and diverse objectives and aims creates friction and deceleration of decision making. Comprehensive national defence can be understood as a complex endeavour [2]. These are endeavours in which there are two or more actors present and where one or more of following conditions exists: the actors have a degree of common intent; the actors are operating at the same time at the same space; and, actions taken by an actor can come conflict with those taken by other actors (Ref. [11], p.29). Therefore, the concepts of C2 approach and of agility (Ref. [17], p. 2-3) are useful tools to understand the ways how to enhance the readiness to cope with changes and accelerate the decision making in complex networks like CND system.

The SAS-085 working group defined agility as capability to successfully effect, cope with and/or exploit changes in circumstances. (Ref. [17], p 9-1) The working group uses six enablers of agility, identified by Alberts and adjusted by SAS-065 working group: responsiveness, versatility, flexibility, resilience, innovativeness and adaptability (Ref. [1], p. 9).

The C2 relationship between participating actors can be described through three dimensions: allocation of decision rights to the collective; patterns of interactions among participating entities; and distribution of information across participating actors [11].

The allocation of decision rights to the collective reflects the actual rights exercised by the entities in a complex endeavour. This allocation can be the result of explicit or implicit laws, regulations, roles, and practices or it can be as a result of emergent behaviour. The allocation of the rights of participating entities to the collective can likewise be explicit, implicit or emergent. An allocation of a right to the collective refers to the degree to which individual entities have given up their respective rights for the benefit of the endeavour as a whole [11].

Patterns of interaction among participating actors are a function of their respective abilities and willingness to interact as well as the opportunities they have as a result of the actual occurrence of interactions and collaborations. Interactions are enabled and their quality is enhanced by the ability to have (face to-face or virtual) meetings, the connectivity of the infostructure, and the degree of interoperability that exists between and among a set of participants (technical, semantic, and cooperability) [11].

Distribution of information across participating actors refers to the extent to which the information needed to accomplish required tasks is available to each participant [11].

Based on these three dimensions, the SAS-065 study recognises five C2 Maturity levels: conflicted, de-conflicted, coordinated, collaborative and edge (Figure 16-1).

Conflicted C2: There is no collective objective among the actors. C2 exist only inside the participating actors.

De-conflicted C2: The objective of the actors is to avoid of adverse cross-impacts between and among the participants by partitioning the problem space. There is limited information sharing and interactions between actors focusing on recognition of potential conflicts in attempting to avoid them.

Coordinated C2: The objective is to increase overall effectiveness by seeking mutual support for intent, developing relationship and linkages between and among actors' plans and actions to reinforce or enhance the effects, some initial pooling of non-organic resources, and increase sharing in the information domain to improve the quality of information. It involves development of certain common intent and an agreement to link actions being developed by the individual actors.

Collaborative C2: The objective is to develop significant synergies by negotiating and establishing collective intent and a shared plan, establishing or reconfiguring roles, coupling actions, rich sharing of

non-organic resources, some pooling of organic resources, and increasing interactions in the Social Domain to increase shared awareness. This approach to C2 involves more than common intent; it involves the collaborative development of a single shared plan.

Edge C2: The objective of Edge C2 is to enable the collective to self-synchronise. The ability to self-synchronise requires that a rich, shared understanding exists across the contributing elements. This, in turn, requires a robustly networked collection of entities with widespread and easy access to information, extensive sharing of information, rich and continuous interactions, and the broadest possible distribution of decision rights. Self-synchronisation includes self-organisation. Thus, entities or collections of entities can look and behave as if they are employing other approaches to C2. The key differences are: In Edge C2 the rights to decisions are broadly distributed even when it appears that decisions are being made by a limited set of individuals or entities. This is because other entities maintain their decision rights. In Edge C2, patterns of interaction are dynamic and reflect the confluence of mission and circumstances. The resulting distribution of information is emergent as a function of the emergent decision-related and interaction-related behaviours.

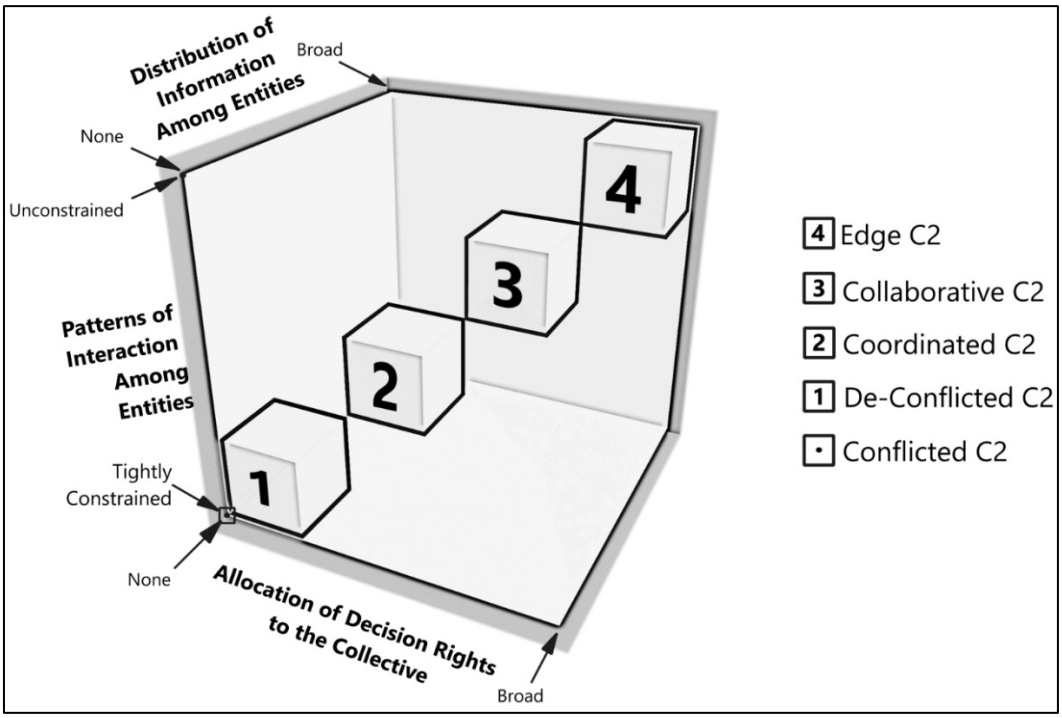

Figure 16-1: C2 Maturity Model: Source: SAS-085.

There is no evidence that a higher maturity level is automatically better, but there is always the optimal C2 solution. Higher maturity level means also that more resources (people, time) should be allocated for coordination and synchronisation activities. Higher C2 maturity level also sets higher requirements for the communication and information sharing equipment as well for the operational and informational security. In addition, at the higher maturity levels the quality requirements (knowledge, skills, attitudes) for individual actors will rise significantly.

Today's military organisations have evolved to be well adapted for mission challenges that are complicated and relatively stable (Ref. [17], p 2-3). Comprehensive national defence tasks will introduce for all stakeholders problems that are not only complicated, but complex. Findings from Phase I studies (Belgium, Estonia, Latvia, Norway, UK) demonstrate that existing agency-centric solutions are mainly able to act on C2 maturity levels 0-2 (conflicted, de-conflicted, and coordinated C2) in inter-agency cooperation [17].

As seen from the example of TRJE18 [11] (Norwegian case study), it can be sufficient in a case of complicated "single lane" events . It is not clear, is it sufficient in solving "multi-lane" events . For example, findings from CD wargame carried out as part of a project "Manticus Apollo" demonstrate, that facing complex "multi-line" problems, the participating actors tends to develop additional intra-agency coordination and information sharing nodes in addition to formal, agreed nodes [7] It may indicate the need for more mature C2 levels to solve the CD situations. The wargame also indicates that if such additional nodes are established only during the exercises or real-life events and not practiced before, the actors may lose the situational awareness or ability to react timely to the events.

16.2.4 Actors and Stakeholders

Stakeholders can be defined as "…any group or individual who can affect or is affected by the achievement of the organisation's objectives (Ref. [11], pp. 9, 18, 23, 36). Based on the broad definition of the comprehensive defence it is easier to list those who are not stakeholders than describe the variety of groups, organisations, and persons, who are affected by the CD. In other words, CD will affect all members of society, which makes robust public relations an important element of CD. This study will focus on actors of the comprehensive defence. Actors of the CD are the persons and organisations who are not only affected by the CD, but have also responsibilities or will to act, have objectives to achieve in the context of CD, or have capabilities and resources to participate in problem solving.

Comprehensive national defence requires an orchestrated and targeted actions by actors, including governmental executive and non-executive agencies, regional and local governments, for-profit and non-profit organisations providing vital services, NGOs and others (Table 16-1). National case studies pointed out differences between these actors in terms of goals, structures, working practices and domains of activity [11].

Table 16-1: Three Main Groups of Actors can be Identified: Public Sector, Private Sector and Civic Sector Actors.

Public Sector	Private Sector	Civic Sector
Government Ministries (defence, internal affairs, foreign affairs, health, communications, etc.) State executive agencies (Defence Forces, police, rescue services, home guard, etc.) Local governments	Businesses Industry For-profit entities	Foundations Charities NGOs Civic groups Individual citizens

By the focus of their interests, these groups can be divided into international, state-level, regional and local actors.

All the actors differ from each other not only because of different objectives and working culture, but also by the organisational design. Some of them have developed hierarchies, allowing to participate in activities at state, region, and site levels. Others have flat structures, which may set the limits to the participation in crisis management at the regional level. Also, the allocation of powers in every participating organisation is different: there are centralised organisations with decision authorities at the top management only, but also decentralised ones.

As seen from case studies, there are different legal inter-agency cooperation mechanisms in place, mainly at the state level of decision. Governmental Security Council and the Crisis Council (Norway), National Security Committee and Crisis Committee of Government (Estonia), National Security Council (Belgium),

Crises Management Council (Latvia) are the examples of such cooperation. Typically, such coordination bodies consist of ministers or deputy ministers and heads of key government agencies. Their responsibilities are limited to coordination of ministry or agency level planning, or synchronising crisis management effort of different ministries and appointing the lead ministry for the crisis or emergency management. As such bodies usually do not have organic analytical and planning capabilities, they rely heavily on capabilities of the participating ministries or agencies. Typically, the lead ministry or agency is responsible for establishing the work procedures and standards. Therefore, there are multiple standards for participating agencies to know and follow.

The principle of a lead agency is used also for the inter-agency cooperation at the regional level. In some cases (Belgium, Norway) it relies on administrative structures of the state, e.g., province; in some cases (Estonia) it relies on the regional units of the state agencies (police, rescue service, defence forces). However, if participating agencies use different geographical areas of responsibility (e.g., Estonia), it creates additional challenges for the cooperation. Also, as seen from case studies, the scope of command authorities and decision authority at the same level of management may differ in different agencies, causing additional frictions in cooperation.

Case studies exemplify relatively well established site-level inter-agency cooperation procedures and practices in solving simple emergencies. As a lead-agency approach is used, there are still too many different cooperation procedures and practices, which may create problem in the situations where the transfer of authority or change of lead agency must occur.

16.2.5 Phases of Crisis Management

The official NATO Crisis Management Process (NCMP) has seven phases: indication and warnings, assessment of situation, development of recommended response options, planning, execution of council (NAC) decisions and directives, transition, and termination of NATO's crisis management role (Ref. [15], p. 3-6). As stated in the AJP-01, this process is designed to allow NATO staff and committees to coordinate their work. Focus on high-level political decision making and on possible threats with significant international impact makes NCMP as a framing construct unusable within the scope of CD.

To describe the crisis management process and the role of the combined headquarters in the crisis management, the more generic three-phase crisis development model of W. Coombs is used. [6] The pre-crisis phase consists of signal detection, prevention, and preparation. The crisis phase covers recognition of trigger events and response. The post-crisis phase consists of recovery, information sharing and learning processes [5]. The context for combined headquarters is, then, a crisis management process that is divided into a three main phases: preparatory phase, crisis-resolution phase and recovery phase.

The preparatory phase consists of activities related to preparation for possible crises and prevention of predictable crises. According to the concept of escalation, the preparatory phase takes place in peace time (tier I), when actors are working within the peacetime legal and institutional frameworks. The preparatory phase is also the key to successfully managing possible future crises. Threat assessment, risk evaluation, mapping the possible crises, preparing plans to counter the crises, identifying the needed capabilities, and building and maintaining them are just a shortlist of main activities that should be performed during the preparatory phase. Executive agencies and services tend to deal with the crisis when it occurs, underestimating the value of systematic and coordinated preparations. Threat assessment and initial risk analysis can be performed agency-based, but to prepare for the complex crisis, a complex view is needed to identify and understand possible spill over effects. Therefore, good inter-agency cooperation is needed in planning and acquiring needed capabilities, and perhaps most importantly – in developing the shared situational awareness system.

The crisis-resolution phase is typically linked to the recognition of the trigger event [6] and consists of different activities to resolve the crisis. As is evident from different studies [8], the trigger event is not always easy to identify. The trigger may be some significant event, threat, or perception of such an event, or understanding that some previous arrangement or modus operandi is no longer viable. Depending on the nature and intensity of events, the crisis response may require tier II-IV activities. As legal and procedural frameworks change from tier to tier, escalation constitutes the biggest challenge for inter-agency cooperation. The crisis-resolution phase is characterised by high operation tempo and unpredictability. Traditionally, such an environment is associated with need for the more centralised management. [8] Theoretically, centralisation can speed up the decision-making process. However, a more centralised C2 system is also more vulnerable and centralised systems are more sensitive to the information overload. Therefore, finding the right balance between the swiftness of action and resilience of command is important.

The recovery phase could be seen as return to a pre-crisis situation, albeit only conditionally. Depending on the extent and type of damage caused by the crisis, restoration of the pre-crisis status quo is not always possible. In such case, the end of crisis is tied with the acceptance of new reality. In principle, the recovery phase consists of the return to a tier I legal and institutional arrangements, physical and psychological recovery, but also learning from the crisis and reconstituting the used capabilities. The beginning of the recovery phase is conditionally identified by the restoration of pre-crisis legal and institutional regime. There is no clear line between recovery and preparatory phase, as the recovery phase just slowly fades away.

16.3 COMPREHENSIVE DEFENCE HEADQUARTERS AND ITS MAIN OPERATING PRINCIPLES

The network of Comprehensive Defence Headquarters is working as decision and control support body for crisis managers at all three decision-making levels. It assists and supports allocated or subordinated units in fulfilling their tasks and shares the information with other organisations and society. The structure and operating principles of the CDHQ remain the same at all levels. The CDHQ is designed to encompass all required skills and competencies to prepare for the crises and to resolve the crises. The CDHQ structure and SOPs are based on functions, tasks and capabilities agreed between the participating agencies. A universal structure, working processes and operating principles, as well the common vocabulary and mental models, will reduce the friction in inter-agency cooperation and therefore increase the responsiveness and flexibility of actions. Also, a combined approach ensures the unity and continuity of command, especially during the resolution of complex crises. Such a set of state, regional and site-level headquarters would require permanent infrastructure and dedicated and trained personnel, retain limited operational capability round the clock, and be gradually expanded as needed.

The network should be seen as command and coordination support tool, to address the comprehensive defence and crisis management challenges. The main areas of responsibility of the CDHQ are crisis and emergency management, HNS, rear area security and support of military operations as required. It is not meant to replace the existing service or agency-based structures, as these have a critical role in building up and sustaining capabilities and developing the agency-specific knowledge.

16.3.1 Concept of Employment

The concept of employment for CDHQ rests upon delineation of events into “single lane” and “multi-lane” events (Figure 16-2).

“Single lane” events are resolvable by organic means of one security-providing agency or vital service provider (police, rescue, ambulance, power grid operator, etc.). In case of a “single lane” event, the tool employed on site is conceptually seen as agency-specific task force under a field leader. In case of a

"single lane" event, all the event management is done by organic structures of the responsible agency and the CDHQ will not be activated. Of course, any "single lane" event can develop at any time into a "multi-lane" event, in which case CDHQ steps in.

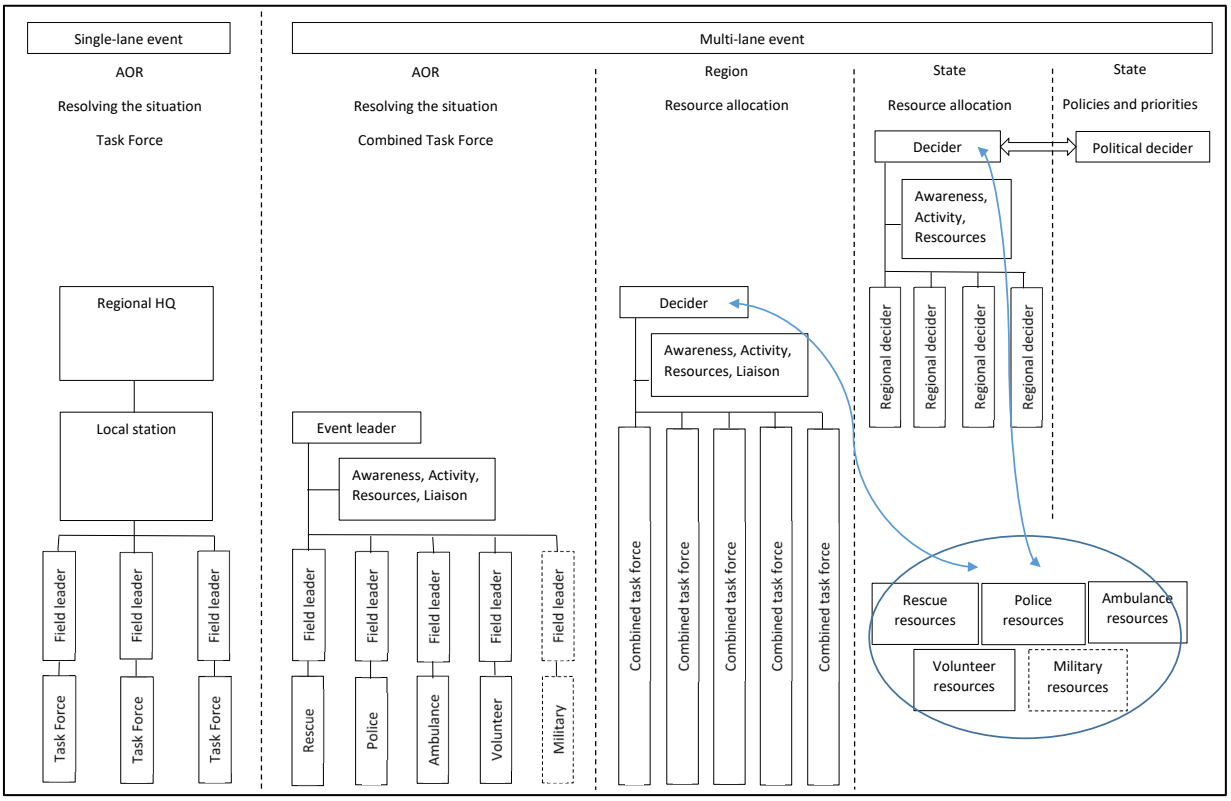

Figure 16-2: Concept of Employment Chart.

A "multi-lane" event is defined as an occurrence resolving of which requires coordinated efforts of many agencies, local governments and/or vital service providers. In case of "multi-lane" event, the tool employed on site is conceptually seen as a Combined Task Force (CTF) where each contributing component has its own field leader, and the field leader from agency responsible for the whole effort is effectively double-hatted as CTF leader. Which agency has the lead responsibility is typically determined by the nature of the event. As the event evolves, lead responsibility may shift; e.g., a mass disturbance implies police responsibility, the use of chemical substance by rioters shifts the centre of gravity to CBRN response where responsibility lies with rescue agency, and further to medical emergency requiring evacuation and treatment of large number of casualties with lead responsibility belonging to ambulance services and then to hospital.

The act of triggering activation an event-level CDHQ could be either the decision of a duty officer at the emergency call centre upon receiving an alert that immediately prompts engagement of more than one agency; or the decision of a "single lane" field leader to ask for support from other agencies. After this decision, infrastructure of CDHQ will be fully activated and relevant agencies, local governments and/or vital service provides alerted to staff their designated contributing and liaison positions at the CDHQ facility.

The role of CDHQ at the event/site-level is to coordinate activities of "parent" agencies – contributors to the CTF – as well as providing necessary horizontal and vertical liaison to other stakeholders (e.g., regional headquarters of contributing agencies, local government, or provider of affected vital services).

At the regional level, the role of CDHQ is overseeing ongoing efforts to resolve several simultaneous events and ensuring allocation and reallocation of resources from contributing agencies available within the region to meet the evolving requirement in the field.

At the state level, the CDHQ maintains situational awareness, oversees activities of regional-level CDHQs, allocates and re-allocates resources at state level to meet the evolving requirement and in accordance with policies, priorities and objectives established by the government-level political decision-making authority (e.g., Crisis Cabinet or alike). National-level CDHQ could also have a responsibility to advise the political decision-making authority in their deliberations regarding policies, priorities, and objectives.

16.3.2 Generic Structure of CDHQ

The generic structure of each CDHQ in the network is the same. It consists of chief of staff and five functional groups: operations, plans, information collection and analysis, support, and public information group (Figure 16-3). Additional functions can be added to a generic structure as needed. The administrative and logistical support responsibilities of staff members and subordinated units remain with their home agencies. Generic tasks of each staff group across the three phases on crisis management are provided in Appendix 16.1.

The Chief of Staff with his expertise is the key person in CDHQ. COS is responsible for overall readiness of the HQ. He coordinates with participating agencies the manning of staff positions, organises staff training, and oversees activities of the planning group during the preparatory phase. During the reaction phase, COS is responsible for timely coordination of HQ activities.

The operations group coordinates ongoing operations, controls the execution of plans, and maintains situational awareness and information sharing with actors. The time horizon for the operations group is typically up to 24 hours.

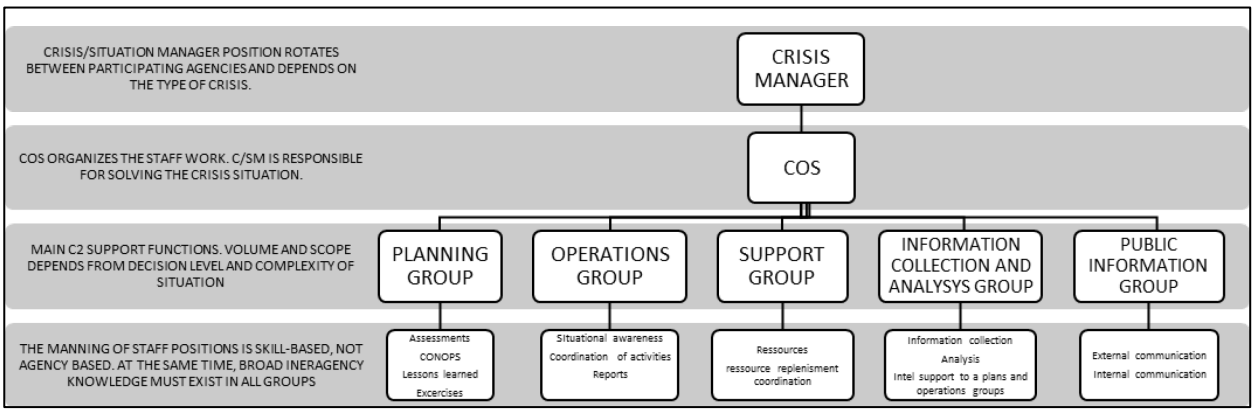

Figure 16-3: The Generic Structure of CDHQ.

The planning group is responsible for mapping possible contingencies and for contingency planning. In addition, the planning group is responsible for preparation and execution of CDHQ staff exercises, and evaluation and lessons learned process, in other words – the very critical tasks at the preparatory phase. During the crisis-resolution phase, the group is responsible for the future planning; i.e., planning the activities further than operations group's horizon – from 24 to 72 hours.

The information collection and analysis group acts as an information fusion and analysis centre, supporting the HQ-s overall situational awareness. As the number of information collection assets owned by the HQ itself is limited, the group relies on information provided by different agencies.

The support group is responsible for the sustainment of operations. It maintains the overview of allocated resources and coordinates the use and replenishment of resources with respective agencies.

The public information group is responsible for sharing information with society. The information sharing includes giving the adequate information about the event, informing population about different restrictions caused by the situation or situation resolution activities, and giving recommendations and instructions to the people. The importance of this function is clear from theoretical works and lessons learned from previous crisis events.

The exact tasks and responsibilities of COS and staff groups differ depending on the level of the CDHQ. Level 1 (site) CDHQs are focusing on resolving of real-time tactical events. Their time horizon is short and main effort is coordinating and synchronising the crisis-resolution activities of allocated units. Level 2 (region) CDHQ is focused on synchronisation of activities on multiple sites. Their time horizon is longer, and their main effort is on sustaining the operations by relocating the units, prioritising activities and coordinating the home agencies' support to participating units. Level 3 (state) CDHQ have the longest time horizon and their main effort is to establish operational and logistic support policies and priorities.

16.3.3 Manning of the CDHQ

The underlying idea of CDHQ is not to create another stovepipe system akin to the Ministry of Emergencies, but to ensure fusion of diverse agency and service experience. For that purpose, "joint crisis management" can be created as a cross-agency speciality to include all alert services (police, ambulance, firefighting), as well as select personnel from non-alert agencies (e.g., veterinary or environmental inspections), local governments, and entities providing vital services – non-profit and for-profit alike.

The CDHQ personnel is envisaged to be effectively double-hatted, retaining their primary designation at home agency, and serving at the CDHQ if the evolving crisis calls for its activation. Personnel to the staff positions is selected by the COS in cooperation with participating agencies based on previously approved job descriptions and staff SOPs. It is important that selected staff member is subject matter expert of a specific field related to the home agency but also a generalist able to understand comprehensive defence and to work in inter-agency environment.

The key means to ensure interoperability via necessary skills and knowledge of staff procedures and tools is a professional development training program that should be a mandatory prerequisite for being appointed to a position in combined HQ. In this way, preparedness to serve at the combined HQ should be seen as additional professional qualification, rather than separate, stand-alone profession.

From the readiness perspective, there should be a rather small permanent staff assigned to each standing CDHQ, with enough pre-assigned personnel from stakeholder agencies to man the staff positions when the CDHQ is activated. At least the COS should be permanently assigned to ensure the coordination of contingency planning and CDHQ staff training at the preparatory phase. The number of other permanently assigned staff depends on the level of CDHQ and the complexity of the area of responsibilities. During the reaction phase, the CDHQ should be able to work on 24/7 regime. To sustain such regime in an uncertain time period, at least three shifts of the staff members should be previously trained for each staff position.

From the functional perspective, relevant personnel at stakeholder agencies should be trained to work at the CDHQ and directed to fulfil the contingency planning and coordination function during the preparatory phase. That should cover also coordination of capability acquisition and joint training.

16.3.4 Authority and Competence Within the CDHQ

Every CDHQ supports the appointed crisis manager or emergency leader. CDHQ relies on its activities on the authority and powers granted to that Crisis Manager (CM). To execute assigned tasks, the CM must have command authority over the assigned units at least on a level similar to TACOM[1] or TACON[2] in a military system. These authorities may differ at each decision level. In classical military headquarters, cooperation with other actors is built on liaison teams. In CDHQ the inter-agency cooperation is built on permanent or assigned staff members, who are acting as subject matter experts and also as a liaison with home agency, if needed. All staff groups have representatives from agencies participating in resolving the situation.

In terms of proficiency, personnel assigned to different levels of combined HQs should fall under one of the following broad qualifications:

- **Junior joint crisis manager:** This level training should be given to all officers of alert services with intra-agency training of field leader, and select personnel from local governments and providers of vital services. After completion of training, they can assume positions at the site-level HQs as functional specialists or liaison to local government or vital service provider.
- **Joint crisis manager:** After completion of follow-on training, the recipients can work as Chiefs of Staff or duty commanding officers at site-level HQ, functional specialists at regional-level HQ or liaison to local government or vital service provider.
- **Senior joint crisis manager:** After completion of follow-on training, the recipients can work as Chiefs of Staff or duty commanding officers at regional HQ or functional specialist at state level HQ.
- **Chief joint crisis manager:** After additional training, the select few qualify as Chief of Staff or duty commanding officers at the state-level HQ.

16.3.5 Area of Responsibility (AOR)

Within the concept of combined headquarters, three levels – site, regional and state – have been defined. Areas of responsibility of site and state-level CDHQs are almost self-evident: the entire country for the latter, and immediate location of the emergency event for the former. Defining regional-level AOR proves more challenging. As exemplified in Phase I case studies, territorial boundaries of responsibility within different agencies (rescue, police) and services (ambulance) do not coincide with each other and often not even with administrative divisions of the country (province or county). On one hand, it may seem reasonable to try to forge an agreement between all stakeholders to align their divisions, but likely political and bureaucratic obstacles – leaving aside the one-time cost of such a realignment – would probably rule this option unfeasible, at least in short term.

As an alternative, the authors of this chapter suggest a different organising principle: reaction time. Assuming that hubs for different services – police or fire stations, or ambulance depots, for instance – are not co-located and may not even be located in the same geographic location (for instance, not every municipality has a major hospital), instead of distance to the scene, the critical parameter becomes time from receiving the alert call to arrival to the scene. If defined in temporal terms (vice spatial), the exact location of response assets becomes irrelevant as long they can respond within the established time limit.

[1] The authority delegated to a commander to assign tasks to forces under his command for the accomplishment of the mission assigned by higher authority [10].

[2] The detailed and, usually, local direction and control of movements or manoeuvres necessary to accomplish missions or tasks assigned [10].

16.3.6 Interoperability and Principles of Information Exchange

To ensure the interoperability between different actors and decision levels, three main mechanisms are used: standardization of procedures and reports, standardization of communication and information exchange equipment, and standardisation of skills and knowledge through common training. The same Standard Operating Procedures (SOP), orders and report formats should be used in all CDHQs regardless of level. The same formats should be used also for the interaction with participating agencies.

Communication and information exchange equipment (voice and data) should enable the coordination and direction of activities with all participating agencies in a timely manner. The development of requirements for and procurement of such systems are agency-based decisions and therefore the problem of compatibility of CIS should be addressed in concerted manner. Technical interoperability can be achieved either through the joint inter-agency procurement of the CIS equipment or by deliberately relying on capabilities of one of the main actors.

The CDHQ's organic data collection capabilities are limited. To ensure the ability of the CDHQ to maintain situational awareness and react to the changes on the ground, it must rely on data and information collected by contributing agencies. Cross-use of databases of different agencies may give rise to legal and security problems in terms of protecting sensitive or classified data and privacy of the citizens. As national regulations differ, this *problematique* should be addressed separately outside of the scope of this study.

16.3.7 Critical Routine Processes

To support the functioning and ability to fulfil required tasks, a few critical routine processes should be executed in the CDHQ through all three phases of crisis management: joint contingency planning, maintaining the situational awareness (including about the resource availability) and ensuring CDHQ readiness.

Joint contingency planning supports the CDHQ readiness to resolve crises. It covers the identification and analysis of possible crises and emergencies, coordination of agencies' contingency planning, evaluation of agencies' plans to counter the emergencies, and assessment and harmonisation of the required capabilities and resources. Joint contingency planning should serve as the basis for synchronising the agency-based procurement programs. Joint contingency planning can be based on NATO-agreed COPD process, modified to accommodate the existing emergency planning systems. The developed contingency plans, as well the risk and threat assessments, must be evaluated periodically, to ensure compatibility with existing capabilities and resources, as well as to synchronise the plans with the corresponding plans at other decision levels.

Maintaining situational awareness is another critical process in the CDHQ. It consists of collection of information for identifying possible trigger events, as well as monitoring the availability and quality of agency-based capabilities.

Maintaining operational readiness of the CDHQ and evaluation of the contingency plans requires individual as well as collective training and rehearsals. Therefore, professional development courses to develop and expand the pool of qualified joint crisis managers need to be conducted on regular basis. Likewise, regular joint exercises should be planned and executed. Crisis management experts have pointed out that the minimum frequency for such exercises could be at least once a year [6].

16.4 MAIN CAPABILITIES, TASKS AND READINESS REQUIREMENTS OF COMBINED HQ

16.4.1 CDHQ Main Capabilities

To describe the CDHQ main capabilities and tasks, the NATO-agreed capability hierarchy [11] is used. The capability hierarchy is modified to suit the comprehensive defence tasks and requirements, and from the

original seven categories, only six are used. The category "Project" is omitted as not applicable to CD. Categories "Engage" and "Protect" are linked together. Depending on the level of the HQ (state, region, site) the scope of capabilities may slightly differ.

Category **Prepare** consists of capabilities to establish, prepare, and sustain sufficient presence at the right time, including the ability to assemble responders, through appropriate and graduated readiness, to meet any requirements, keeping sufficient flexibility to adapt to possible changes in the environment.

- **Subcategory R1 (Force preparation):** As individual and agency-specific collective training is the responsibility of respective agencies, CDHQ should have capability to prepare and conduct joint inter-agency exercises in full range of the tasks assigned for the CDHQ at least once per year. The COS is responsible for the CDHQ personnel individual training and CDHQ collective training.
- **Subcategory R2 (Capability development):** CDHQ, specifically its planning group, should have the capability to conduct the threat and risk analysis, to conduct contingency planning and to identify minimum required responders to counter the foreseeable contingencies, as well as identifying the emerging requirements. Capability to act together coherently, effectively, and efficiently to achieve the objectives.
- **Subcategory R3 (Advisory and compliance):** Capability to identify, analyse and rectify lessons derived from exercises and operations and to give the input to an agency-based procurement requirements and capability to develop programs. Capability of ensuring, assessing compliance with policies and regulatory requirements and providing advice on shortfalls and risks. Also, capability to evaluate assigned responders to ensure attainment of defined performance or operational standards.
- **Subcategory R4 (Building Partnership):** Capability to establish and develop the long-term partnership with governmental agencies, for-profit and non-profit organisations, local government, and population in the area of responsibility.
- **Subcategory R5 (Generation):** Generation of pool of responders is mainly the responsibility of contributing agencies.
- **Subcategory R6 (installation support):** HQ relies on the capabilities on one of the existing agencies and does not have own installation support capabilities.
- **Subcategory R7 (Corporate Management and Support):** Capability to manage the information and knowledge to ensure optimal utilisation of corporate information resources across domain and between teams.

Category **Prepare** is clearly linked with the crisis management preparatory phase. The main workload on this phase is on the COS and the planning group.

Category **Engage** consists of capabilities to perform tasks, which contribute directly to the achievement of mission goals within the context of comprehensive defence, crisis, and emergency management.

- Taking into account the main mission and principal tasks of the CDHQ, the subcategories E1 (joint manoeuvre) and E2 (Joint fires) are not applicable.
- Subcategory E3 (Non-kinetic engagement):
- Capability to direct information content, dissemination, and audience in order to influence the perceptions, attitudes and behaviour of selected individuals and groups.
- Capability to coordinate information functions, integrating STRATCOM into the planning and decision-making process.
- Capability to coordinate and cooperate with other actors in the area of responsibility.

Category **Sustain** consists of capabilities to plan and execute the timely support and sustainment of assigned responders. CDHQ with no organic logistic support units has only coordinating powers and relies on the capabilities of home agencies.

- Capability to know the status of assigned responders, future operational requirements and to coordinate the sustainment and management issues with the home agencies

Category **Consult, Command and Control** consists of capabilities to exercise authority over and direct assigned responders in the accomplishment of the mission. Includes the capability to communicate and coordinate with other actors, which are present or involved in the operational area and effective information exchange with the superior and subordinated HQ-s, capability to plan, employ and coordinate with other actors.

Category **Protect** consists of capabilities to minimise through Force Protection the vulnerability of personnel, facilities, materiel, and activities to any threat and in all situations.

- **Subcategory P1 (Security)**: Capability to ensure that designated information, materiel, personnel, activities, and installations are protected against espionage, sabotage, subversion, and terrorism, as well as against loss or unauthorised disclosure. Information security against espionage, loss or unauthorised disclosure should be provided by organic means of the CDHQ. All other needed capabilities in this area should be covered by other agencies.
- **Subcategories P2 (Defence)** and **P3 (Hazard Mitigation)** should be fully provided by contributing agencies.

Category **Inform** consists of capabilities to establish and maintain the situation awareness and level of knowledge required to allow CM to make timely and informed decisions.

- **Subcategory I1 (Collect)**: CDHQ may have organic capability to collect timely and accurate information from publicly available sources (I1.5. Open Source). In other areas (I1.1. Acoustic, I1.2. Human, I1.3. Imagery, I1.4. Measurement and signature, I1.6. Signals) it relies on capabilities of contributing agencies and other actors.
- **Subcategory I2 (Processing)**: Capability to receive, convert and fusing data and information from all available sources into relevant and usable intelligence/knowledge, decision support and situational awareness products by collation, evaluation, analysis, integration and interpretation through fusion and collaboration.
- **Subcategory I3 (Dissemination)**: Capability to distribute timely data, information, intelligence and specialist and all-source analysis, in an appropriate and accessible form, across and between networks as required.

16.4.2 Readiness of the CDHQ

The readiness of the CDHQs to quickly assume the responsibility for resolving the crisis relies on three pillars: previously selected and technically prepared working places (including voice and data communications); permanently appointed and qualified personnel; and standardised working procedures.

CDHQ has three states of activation: dormant, partial, and full.

Dormant state describes the status of CDHQ in escalation Tier One. The CDHQ facilities, communications and information systems are up and running, appointed personnel are trained to meet the qualification requirements, and contingency plans are refreshed on a regular basis. The main workload is on the Chief of Staff.

Partial activation is used in escalation Tiers Two and Three to react to the crises when participation of all assigned agencies is not necessary either due to specific characteristics of the crisis or its limited impact.

Fully activated CDHQ is used in escalation Tiers Two and Three to react to complex or large-scale crises.

16.4.3 Minimum Infrastructure Requirements

The CDHQ as the inter-agency cooperation framework will not necessarily need its own separate infrastructure but could build upon the already existing facilities of one of the participating agencies, expanded and upgraded as required to support the requirement.

The required infrastructure can be divided into physical and cyber components. At a minimum, the physical infrastructure must consist of working places for the CM and staff members, briefing room or rooms, voice and data connections as well the appropriate physical security measures (e.g., controlled access). The cyber component should allow for secure, seamless, and real-time access to databases and intra-agency communications networks of all participating actors.

16.5 SUMMARY AND CONCLUSIONS

Existing real-life comprehensive defence systems can be described as complex endeavours consisting of a large number of diverse actors with often conflicting objectives and perceptions operating under ambiguous command lines, which creates challenges in implementing the common tasks. Therefore, collaboration between stakeholders with underlying C2 mechanisms, joint financing mechanisms, joint plans, and joint strategies is indispensable.

A uniform approach is required to describe and compare the elements of the diverse universe of concepts, actors and standard operating procedures across multiple countries and different institutional frameworks. The approach outlined in this study rests on five supporting concepts. The concept of escalation underpins the institutional dynamic of authorities and actions within the context of crisis management effort. A generic framework of levels of decision making enables the activities of military and non-military actors to be grouped and organised in a comprehensive manner. The concept of command and control agility addresses the flexibility and speed of coping with uncertainties and complexity of possible crises. The concept of crisis management phases deals with the volatility and unpredictability of the crisis and offers a holistic framework within which to address the continuum of events from pre-crisis to post-crisis status quo. Finally, the concept of stakeholders addresses the diversity and complexity of actors in the comprehensive defence system.

National case studies highlight that the dynamics and complexity of modern crises requires a flexible and agile crisis management system, which can only be built on common situational awareness and close cooperation between the main actors of comprehensive defence. A solution to this challenge can be the network of combined Comprehensive Defence Headquarters. Such a set of state, regional and site-level headquarters would require permanent infrastructure and dedicated and trained personnel, retain limited operational capability round the clock, and be gradually expanded as needed. The main areas of responsibility of the CDHQ are crisis and emergency management, HNS, rear area security and support of military operations as required. The role of CDHQ at the site level is to coordinate activities of contributing agencies as well as providing necessary horizontal and vertical liaison to other stakeholders. At the regional level, the role of CDHQ is overseeing ongoing resolve efforts of several simultaneous events and ensuring allocation and reallocation of resources from contributing agencies available within the region to meet the evolving requirement in the field. At the state level, the CDHQ maintains situational awareness, oversees activities of regional-level CDHQs, allocates and re-allocates resources at state level to meet the evolving requirement and in accordance with policies, priorities and objectives established by the government-level political decision-making authority. A national-level CDHQ could also have a responsibility to advise the political decision-making authority in their deliberations regarding policies, priorities, and objectives.

The generic structure of each CDHQ in the network is the same. It consists of a chief of staff and five functional groups: operations, plans, information collection and analysis, support, and public information group. The CDHQ personnel is envisaged to be effectively double-hatted, retaining their primary designation at home agency, and serving at the CDHQ if the evolving crisis calls for its activation. The generic structure will bring about standardisation of procedures and reports, standardisation of communication and information exchange equipment, and standardisation of skills and knowledge through common training, ensuring interoperability between different actors and decision levels. Through all three phases of crisis management, CDHQ must execute joint contingency planning, maintaining situational awareness (including resource availability) and ensuring required readiness. The required capabilities of the CDHQ are established using the NATO-agreed capability hierarchy across the categories "Prepare", "Engage", "Sustain", "Consult, Command and Control", "Protect", and "Inform". The readiness of the CDHQs to quickly assume responsibility for resolving the crisis relies on three pillars: previously selected and technically prepared working places (including voice and data communications); permanently appointed and qualified personnel; and standardised working procedures.

Planning for, and conduct of operations in a complex, multi-domain environment with involvement of different military, paramilitary and non-military organisations, to include countering hybrid threats, requires a coherent conceptual framework to ensure shared understanding of missions, tasks, capability requirements and concepts of operations. A network of CDHQs, working as command, control, and decision support body for crisis managers, as well as coordination and de-confliction framework whilst using unified procedures, operational language, communication means and shared situational awareness in addition to the common training will ensure preparedness to act and timely respond to unwanted events.

16.6 REFERENCES

[1] Alberts, D.S., and Hayes, R.E. (2003), "Power to the edge", DoD CCRP Publications Series, Washington, DC, USA.

[2] Alberts, D.S., and Hayes, R.E. (2007), Planning: Complex Endeavors, DoD CCRP, Washington, DC. http://www.dodccrp.org/files/Alberts_Planning.pdf

[3] Bryson, J. M. (2004), "What to do when stakeholders matter: stakeholder identification and analysis techniques", Public Management Review, Vol. 6 No. 1, pp. 21-53.

[4] Centre for Civil-Military Relations (CCMR), (2006), Unpublished proceedings of seminar "Roles and Missions in the national defense of Azerbaijan", 24 – 28 April, Baku, Azerbaijan.

[5] Coombs, W.T. (2006), "Code red in the boardroom: Crisis management as organizational DNA", Westport, CN: Praeger.

[6] Coombs, W.T. (2012), Ongoing Crisis Communication: Planning, Managing, and Responding. Thousand Oaks, CA: Sage.

[7] Dieves, V. (2020), "Manticus Apollo wargame and its results", Sõjateadlane. Estonian Journal of Military Studies vol.15, pp. 147-176. Kaitseväe Akadeemia (in Estonian).

[8] Hart, P.'t., Rosenthal, U., and Kouzmin, A. (1993), "Crisis decision making: The centralization thesis revisited", Administration & Society, Vol. 25, Issue 1, p. 12.

[9] Murumets, J. (2007), "Renewed national defense planning and management: Capability-based planning, programming, budgeting and execution system for small states", Proceedings of the Estonian National Defense College 7/2007. Tartu University Press.

[10] NATO AAP-6. NATO Glossary of Terms And Definitions (2013), North Atlantic Treaty Organization NATO Standardization Agency (NSA).

[11] NATO STO (2010), "NATO NEC C2 maturity model", SAS-065, DoD CCRP Publication Series, Washington, DC, USA.

[12] NATO STO (2021), "Conceptual framework for comprehensive national defence system", Interim report of the SAS-152 study: Review of literature, case studies and preliminary findings, NATO STO Technical Report STO-TR-SAS-152-Part-I. Pre-release. NATO STO, Neuilly-sur-Seine, France.

[13] North Atlantic Treaty Organization (NATO) (2007), "NATO Bi-SC Directive 80-90, NATO tasks list", 19 November 2007.

[14] North Atlantic Treaty Organization (NATO) (2012), ATP-3.2.2 C-2 Edition B Version 1 Annex C NATO UNCLASSIFIED December 2016.

[15] North Atlantic Treaty Organization (NATO) (28 February 2017), 2017 AJP-01. Allied Joint Doctrine. Edition E version 1.

[16] SH/PLANS/JCAP/FCP/15-310118 (2015) Bi-SC Capability Hierarchy.

[17] STO NATO (2014), "Command and Control (C2) agility", Task Group SAS-085 Final Report, STO-TR-SAS-085, NATO STO, Neuilly-sur-Seine, France.

Appendix 16-1: CDHQ GENERIC TASK LIST

Staff Groups	Main Tasks of the Staff Groups in Different CM Phases		
	Preparatory Phase	**Crisis-Resolution Phase**	**Recovery Phase**
COS	• Coordination of manning the HQ positions with competent personal • Evaluation and training of dedicated personal • Establish the SOP and HQ working plan and battle rhythm • Coordination with other agencies CM planning processes • Supervision of the planning group work • Organisation of staff trainings and plan rehearsals • Leading the preparation of the physical working space • Including security and cyber security • Maintaining the appropriate readiness level of HQ	• Maintaining the HQ battle rhythm • Maintaining the manning of the HQ with competent personal in cooperation with home agencies • Supporting the CM on preparing and executing crisis-resolution plans • Ensuring the needed working conditions of the HQ, including security and cyber security	• Manning the HQ with competent personal • Coordinating the HQ work • Coordinating the lessons learned process
Operations group	• Situational awareness is maintained on need basis, typically during the staff exercises. Connections to link with the other agencies are ready • Keeping the HQ battle book • Preparing SITREP on need basis • Preparation of orders on need basis • Coordination of activities with agencies and other CD HQ-s	• Maintaining situational awareness 24/7 including at least police, rescue, medical, life-critical infrastructure, etc. • Keeping the HQ battle book • Daily SITREP, INCREP, CONTACTREP, QUICKSITREP • Preparation of orders • Coordinating activities of allocated and subordinated units • Coordination of activities with agencies and CD HQ-s	• Situational awareness is maintained on need basis, typically during the staff exercises • Keeping the HQ battle book • Preparing SITREP on need basis • Preparation of orders on need basis • Coordination of activities with agencies and CD HQ-s

Staff Groups	Main Tasks of the Staff Groups in Different CM Phases		
	Preparatory Phase	**Crisis-Resolution Phase**	**Recovery Phase**
Planning group	Preparation of threat and risk assessments and contingency plans in cooperation with other agencies, local governments and private sector Evaluating the capability caps Preparing the CM exercises and plan rehearsals as tasked by COS Assessing lessons learned from exercises and plan rehearsals	Preparing the future plans, including recovery plans	Preparation of: Threat and risk assessments; contingency plans; Evaluating the capability caps Evaluating lessons learned from crisis resolution
Information collection and analysis group	Planning and coordinating the information collection to support the contingency planning and to maintain the readiness of HQ Preparing and providing intel updates for operations and planning groups on need basis	Planning and coordinating the information collection; Assessing the collected information Preparing and providing regular intel updates for operations and planning groups	Planning and coordinating the information collection Preparing and providing intel updates for operations and planning groups on need basis
Support group	Maintaining the overview of assigned and available resources Participating in CM contingency planning Coordination of replenishment of resources with agencies	Maintaining the overview of assigned and available resources Coordination of replenishment of resources with agencies Acquiring the additional resources Reassigning the resources between allocated or subordinated units	Maintaining the overview of assigned and available resources Coordination of replenishment of resources with agencies Acquiring the additional resources
Public information group	Participating on CM exercises Preparing the	Preparing the information releases for communities Informing people, local governments, private sector about the additional regulations, restrictions	

Chapter 17 – ADAPTATION OF EMERGING TECHNOLOGIES INTO DEFENCE

Sait Yılmaz
Esenyurt University
TURKEY

17.1 INTRODUCTION

The 21st century can be considered as the revolutionary age of technology. We have seen some major advancements in the field of technology in the last decade and it is still going on at a rapid pace. The technology which is new today will become obsolete tomorrow given the speed with which new concepts and techniques are developed every day. Emerging and disruptive technologies encompass both new technology, and new use of existing technology, which will change the way we or potential adversaries operate. This includes 'game-changing' technology that revolutionises the field, but which could come with risks attached because it is new and untested. In this rising tide of revolutionary technology, the two most popular concepts which have gained the most attraction are AI (Artificial Intelligence) and Biotechnology including Human Enhancement.

AI has allowed us to eliminate the factor of human error from any kind of work. It has led to a huge increase in the demand for artificial intelligence in various fields. How is AI implemented in defence systems? AI is increasingly becoming an integral part of the defence and modern warfare systems. Compared with conventional systems, military systems equipped with AI are capable of handling larger volumes of data more efficiently. Additionally, AI improves self-control, self-regulation, and self-actuation of combat systems due to its inherent computing and decision making capabilities [1]. Its convergence with other related technologies, especially the Internet of Things (IoT) and Robotics, has tremendous applications in defence sectors. AI is deployed in almost every military application, and increased research and development funding from military research agencies to develop new and advanced applications of artificial intelligence is projected to drive the increased adoption of AI-driven systems in the military sector.

The Biotechnology (BT) and Human Enhancement domains have been subdivided into the following areas:

- Virtual reality
- Exoskeletons and neuro-enhancement for Human Enhancement;
- Bioinformatics and biosensors;
- Biomedical technology and medical countermeasures, and
- Synthetic biology for Biotechnology.

The pipeline of biotechnology products likely to emerge over the next decade will probably result in disruptive innovations and significant societal impacts, even though currently it seems to be underestimated in its exploitation in military applications with respect, as a main example, to soldier resilience and survivability. Biotechnology will provide a new source of information for accelerating the development of weapons and equipment. For instance, the application of high-performance bionics and biomaterials could provide a new material basis for weapons and equipment; Human Enhancement Technologies (HETs) are biomedical interventions that are used to improve human form or to function beyond what is necessary to restore or sustain health. HET may enhance physiological, cognitive or social functions.

The world may be on the verge of a significant change in the character of war, or it may not. As is always the case preceding such transformations, there is a great deal of uncertainty about when they will occur and how military forces will need to adapt to remain competitive in the new environment. As the nations approach the dramatic changes that military AI/BT-HET might cause, the national leaders will be confronted with tensions between competing demands: the imperative to prepare forces to fight and prevail against adversaries with these capabilities versus the need to manage the strategic risks and potential costs of arms races. How successful the nation is in maintaining military superiority in an increasingly dangerous world will depend on how smartly the national leaders manage these tensions. In this chapter, we will investigate the possible applications of AI/BT-HET for defence systems and generic concepts to refer to their implications.

17.1.1 Emerging Technologies

The following definitions have been agreed in the context of NATO documents [2]:

> **Emerging:** Those technologies or scientific discoveries that are expected to reach maturity in the period 2020 – 2040; are not widely in use currently or whose effects on Alliance defence, security and enterprise functions are not entirely clear.
>
> **Disruptive:** Those technologies or scientific discoveries that are expected to have a major, or perhaps revolutionary effect on NATO defence, security or enterprise functions in the period 2020 – 2040.
>
> **Convergent:** A combination of technologies that are combined in a novel manner to create a disruptive effect.

Currently, NATO has determined the development maturity of the following seven Emerging and Disruptive Technologies (EDTs). Their potential impact on the military as well as on a wide sphere (if feasible) has been evaluated [2]:

1) Data and Big Data Analytics;
2) Artificial Intelligence and Machine Learning;
3) Autonomy;
4) Space;
5) Hypersonic Vehicles and Missile Defence Technologies;
6) Quantum Technologies; and
7) Biotechnologies and Human Enhancement.

EDTs could range from those that are expensive and challenging to develop – for example hypersonic – to those that are cheap and easily accessible but used in novel ways – for example non-state actors using drone technology in ways which could challenge norms of behavior – to those that disrupt the fundamental operating understanding of our conventional approaches, such as artificial intelligence, quantum computing and sensing.

AI, Big Data, Machine Learning

AI and big data are complementary technologies that are closely linked. As information is a key contribution to big data analytics and AI, data integrity and data quality are fundamental elements in any solution deployed in the military domain or in the civilian sector and must be preserved during all stages of data use (from creation to data exchange, sharing and archiving). For NATO and its allies, a coordinated approach is required for the development and use of AI and big data, based upon open, publicly available, and international standards. Unlike the past, where data services were piggy-backed onto topical projects, these fields now need to become integrated into quality projects in order to achieve common, interoperable platforms which seamlessly connect with existing frameworks.

Autonomy

Autonomy is a domain which, in the Western World, has benefited from major investments, both civil and military. Examples from the civil sector are drones, autonomous cars, and autonomous manufacturing. Within the defence domain, examples of autonomous technology have been in service for many years. Some key issues that require further development in the autonomy domain are man-machine teaming and the degree of human control required, this latter point being influenced by ethical, moral, legal and safety considerations. The impact and inclusion of emerging technologies, especially AI and big data, require a high level of trust to be built up with respect to how these autonomous system(s) operate and adapt to their environment.

Space

For the Alliance, the dependence on space is currently not matched by the resilience of space assets. On-orbit assets face a particular problem because of Anti-Satellite (ASAT) and space piracy threats and a greater number of defensive and Operationally Responsive Space (ORS) options are needed as a counter. To deal with the space threats, NATO must build up its space expertise and enhance its Space Surveillance and Tracking and Space Domain Awareness capabilities. A particular concern which demands understanding and keen analytical skills being that the exigencies of the Domain can result in effects that mimic attacks by an adversary.

Spectrum and 5G/6G

New generations of cellular telecommunications technology offer economic growth, which is being promoted by governments and commercial companies alike. Growth is forecast to come from the large increases in data throughput capacity that 5G (and later generations of the technology) will provide. Applications (known in the parlance as ‘use cases’) using Artificial Intelligence, Big Data, Autonomy and Robotics, and eCommerce will exploit the benefits of high throughput and low latency. The combination of these new bearer technologies and use cases is an illustration of how converging technologies can have a disruptive effect.

There is intense competition for spectrum, particularly in some of the lower frequency bands. The military must learn to build robust business cases to protect services from interference. Perhaps of even more importance than resilience, is the assurance that service providers can be trusted. However, a key step towards being able to address the aforementioned challenges is to recognise spectrum operations as a new operating domain, in much the same way as Cyber and Space.

Hypersonic Platforms and New BMD Technology

To counter the threat from hypersonic platforms, which could be travelling at speeds of up to Mach 20, NATO and its allies need to address a number of issues.

First, to examine and coordinate the numerous hypersonic platform and technology developments that are taking place within NATO nations, to produce a coherent Alliance strategy that could provide a timely game-changer capability.

To utilise model, simulation, and test flight data to explore the threat flight profile boundaries to enable forward-prediction of engagement zones, use of counterforce, and identify where modification to today’s effector capabilities could yield capability.

The use of hypersonic and cruise missiles requires that defence planning becomes global in nature and coordinated across the Alliance. The increase in battlefield volume requires an equivalent growth in exploitation and fusion of all available sources of intelligence and data.

Quantum Technologies

Globally, this domain is driven by very large public investments, including both in the US and China. Other relevant drivers include: the hype over Quantum Computing (QC) and its potential threat to cryptography which fostered quantum communications, intrinsically secure by the laws of physics and able to detect any eavesdropping attempt.

Computing is the only area in which large companies, such as Google, IBM, Intel, Alibaba, etc., are represented, which is due to the large investments required in this area and to the large, expected impact in the 'Big Data' sector computing. On the other hand, both in sensing and communication domains work is mainly centred in academia, research organisations and in Small and Medium size Enterprises (SMEs).

There is an ongoing convergence of four key technologies that are poised to transform the Information and Communications Technology (ICT) ecosystem. Those technologies are Fifth Generation (5G) cellular, Artificial Intelligence (AI), Data Analytics, and the Internet of Things (IoT). Artificial intelligence represents the use of machines, or computers, to simulate activities thought to require human intelligence. There are different AI methods used by researchers, companies, and governments, including machine learning and neural networks [3].

Bio Technologies and Human Enhancement

Biotechnology has become an increasingly agile platform for developing new types of soldier enhancements. As such, the field offers novel opportunities for improving warfighter survivability on the battlefield. The "dual use" natures of the life sciences and biotechnology, in which the same science and technology base that improves health, promotes innovation, and protects the environment, can also be misused to facilitate a biological attack.

The development of new human augmentation technologies has the potential to change the capabilities of the individual soldier, sailor, or aviator significantly and create integrated human-machine symbiotes of unparalleled capabilities. Furthermore, rapid advances in material, computer, and human sciences, as well as convergence between these fields, is setting the stage to enhance human capabilities and push the human performance frontiers significantly.

17.1.2 National Security and AI

Artificial intelligence (AI) is having a moment in the national security space. AI could trigger World War III (see Vladimir Putin's Statement [4] that leadership in AI will be essential to global power in the 21st century). Artificial intelligence is not a weapon. Instead, artificial intelligence, from a military perspective, is an enabler, much like electricity and the combustion engine. Thus, the effect of artificial intelligence on military power and international conflict will depend on particular applications of AI for militaries and policymakers. The potential promise of AI – including its ability to improve the speed and accuracy of everything from logistics to battlefield planning and to help improve human decision making – is driving militaries around the world to accelerate their research into and development of AI applications.

The defence and security industry is also not spared from the likes of this disruptive technology. It can bring a profound transformation to improving national security, driving economic prosperity, and enhancing public safety. AI has the potential to see beyond the horizon and help personnel in safeguarding national integrity. Already, many countries' defence departments are using AI, robotics, and drone technology in many defence applications. The aim is to build a more autonomous strength, pairing AI-powered systems and robotics with human military personnel to enable faster decisions and better combat results. As they leverage advanced technology to come up with innovative solutions, there are some AI startups that are empowering the defence and security industry [5].

Artificial Intelligence (AI) is a rapidly growing field of technology with potentially significant implications for national security. AI research is underway in the fields of intelligence collection and analysis, logistics, cyber operations, information operations, command and control, and in a variety of semiautonomous and autonomous vehicles [6]. Already, AI has been incorporated into military operations in Iraq and Syria. As such, the United States and other nations are developing AI applications for a range of military functions. Currently, China is primarily focused on using AI to make faster and more well-informed decisions, as well as on developing a variety of autonomous military vehicles [7]. Russia is also active in military AI development, with a primary focus on robotics.

Considered as the 4th Industrial Revolution, Artificial Intelligence (AI) has become a reality in today's world, especially in the military. Even though AI is still at its juvenile stage, it is undeniable that it has the capacity to alter the landscape of the security sector and as a result, it will change the current economic and military balances in the international system. Recognising the potentials of AI, more than 20 countries have announced their national AI strategies, and more states and non-state organisation are taking decisive steps in AI Research and Development (R&D). Many experts argue that AI itself should not be considered as a specific weapon, but it should be seen as "an enabler, a general-purpose technology with a multitude of applications" [8].

For the majority of AI researchers, AI is about making machines capable of mimicking capabilities that are usually associated with human intelligence, such as observing the world through vision, processing natural language or learning [9]. AI is programmed to do something similar, in that a computer senses the world around it, and then processes the incoming information through optimisation and verification algorithms, with a choice of action made in a fashion similar to that of humans [10].

Figure 17-1 illustrates how an autonomous system embedded with AI 'thinks' and makes decisions in this way.

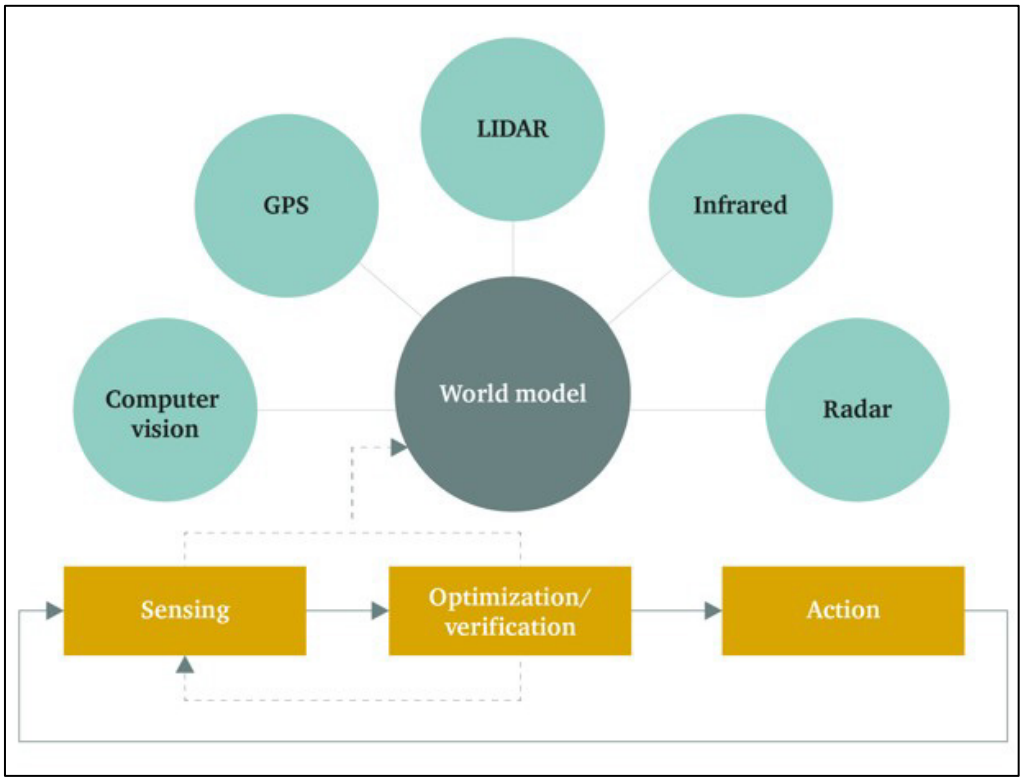

Figure 17-1: How AI of an Autonomous System Works [Hutchins, Cummings, Draper and Hughes (2015)] [11].

While many analysts admit that military AI technology is in a stage of infancy, it is difficult to find an expert who believes that AI will be inconsequential in the long run [12]. However, AI critics point to a number of trends that may minimise the technology's impact. From a technical standpoint, there is a potential that the current safety problems with AI will be insurmountable and will make AI unsuitable for military applications. Some experts believe that the present family of algorithms will reach its full potential in another 10 years, and AI development will not be able to proceed without significant leaps in enabling technologies, such as chips with higher power efficiency or advances in quantum computing.

In computer science, pattern recognition can be divided into various subsections:

- Biometrics: identification of people using e.g., facial, fingerprint and/or iris recognition;
- Linguistics: including language identification, language understanding (e.g., in translating), speech recognition (conversion of the spoken word into text) and voice recognition (identifying the person speaking);
- Textual: e.g., handwriting and character recognition used to convert handwritten or typewritten text into machine-encoded text;
- Gesture recognition: the interpretation of human gestures;
- Activity recognition: the recognition of events; and
- Object recognition (Ref. [2], p. 166).

To better understand the nuances of AI, it is important first to understand the difference between an automated and an autonomous system. An automated system is one in which a computer reasons by a clear if-then-else, rule-based structure, and does so deterministically, meaning that for each input the system output will always be the same (except if something fails). An autonomous system is one that reasons probabilistically given a set of inputs, meaning that it makes guesses about best possible courses of action given sensor data input. Unlike automated systems, when given the same input autonomous systems will not necessarily produce the exact same behaviour every time; rather, such systems will produce a range of behaviours.

Many autonomous systems incorporate AI in some form. Such systems were a central focus of the Obama Administration's "Third Offset Strategy", a framework for preserving the US military's technological edge against global competitors [13]. Depending on the task, autonomous systems are capable of augmenting or replacing humans, freeing them up for more complex and cognitively demanding work. In general, experts assert that the military stands to gain significant benefits from autonomous systems by replacing humans in tasks that are "dull, dangerous, or dirty." Specific examples of autonomy in military systems include systems that conduct long-duration intelligence collection and analysis, clean up environments contaminated by chemical weapons, or sweep routes for improvised explosive devices.

17.2 APPLICATIONS OF AI INTO DEFENCE

17.2.1 Defence Applications of AI

AI is not magic; adopting AI tools is no guarantee of success. But given the role AI is likely to play in future conflict, *not* adopting AI will likely guarantee failure. Therefore, learning how to effectively use AI today – with all of its strengths and weaknesses – will be critical to success on future battlefields. The main reason behind the power of AI to shift the current balances of power relies on the fact that the application of AI in the military will give the states the upper hand in the battlefield, as the machines will be more accurate and faster than humans in logistics, battlefield and decision making. Furthermore, with the help of AI, the military can perform high risk missions for a long period of time, something that cannot be done by humans.

First of all, warfare will be pushed to the limits in terms of time scale. AI's capacity to react on machine speed will accelerate the pace of combat [14]. Whether this development will be beneficial or not is highly contested among analysts [15], [16]. Second, the current military structure and organisations are going to change as new concepts of operations evolve (ex: swarm drones). Third, AI may provide the opportunity to cope with a huge amount of data available for analysis. By addressing this data, AI systems will be able to provide results or solutions that humans may not be able to think about, especially when found in combat.

Visions exist of AI enabling autonomous systems to conduct missions, achieving sensor fusion, automating tasks, and making better, quicker decisions than humans. Most AI systems today are trained to do one task, and to do so only under very specific circumstances. Unlike humans, they do not adapt well to new environments and new tasks. Most of what occurs inside an AI system is a black box and there is very little that a human can do to understand how the system makes its decisions. AI is many years from bearing fruit. AI systems also struggle to distinguish between correlation and causation [17].

Such technologies can be highly relevant for the development of lethal autonomous weapons, enabling the automatic identification and subsequent attack of targets based on the recognition of certain patterns by AI systems. This section focuses mainly on facial recognition technology. Ever since surveillance cameras and biometric identification emerged in the public domain, these technologies have caused concerns relating to their impact on the right to privacy and bodily integrity.

There are many reasons to investigate the potential benefits of AI application to defence systems, but the most relevant is that AI promises to improve the speed and accuracy of just about everything from logistics to battlefield planning and speed in this case is not about the velocity of an airplane or a munition. Speed is about decision making, making the right decisions first and shortening the C2 cycle [18].

The potential military benefits of AI include faster and better decision making, improved ISR and precision targeting, mitigation of manpower issues, and improvements in cyber defence. Although AI has the potential to impart a number of advantages in the military context, it may also introduce distinct challenges. AI technology could, for example, facilitate autonomous operations, lead to more informed military decision making, and increase the speed and scale of military action. However, it may also be unpredictable or vulnerable to unique forms of manipulation. As a result of these factors, analysts hold a broad range of opinions on how influential AI will be in future combat operations. While a small number of analysts believe that the technology will have minimal impact, most believe that AI will have at least an evolutionary – if not revolutionary – effect.

Currently, the NATO has determined the development maturity of seven Emerging and Disruptive Technologies (EDTs), and has evaluated their potential impact on the military and, if feasible, wider sphere [2] (Table 17-1).

Artificial Intelligence and Robotics shall play significant role in number of defence applications such as [19]:

- Image interpretation for target identification and classification.
- Expert systems for diagnosis and maintenance of sophisticated weapon systems such as radars and missiles.
- Robotic equipment can be used to provide precision targeting support and carriage of ammunition and accuracy.
- Camera equipped and shock-resistant platforms to provide fire power remotely are also possible applications.
- Systems for diagnosis and maintenance of sophisticated weapon systems.
- Missile target range and trajectory analysis for evaluation of kill zones, launch time and simulation to assist in qualifying missile performance in various environments.
- Enhanced use of robots for Anti-Improvised Explosive Device, extraction of personnel, firing of guns and other applications.

Table 17-1: Maturity Matrix Timeline.

Years		2010	2020	2030	2040	2050
Emerging (Discoveries)		x	x	x		
Disruptives	Data and Big Data Analytics		x	x	x	
	Artificial Intelligence and Machine Learning		x	x	x	
	Autonomy		x	x	x	
	Space			x	x	
	Hypersonic Vehicles and Missile Defence Technologies		x	x		
	Quantum Technologies		x	x	x	
	Bio technologies and Human Enhancement			x	x	
Convergent				x	x	x

Notes:

Emerging technologies or scientific discoveries that are expected to reach maturity in the period 2020 – 2040; and are not widely in use currently or whose effects on Alliance defence, security and enterprise functions are not entirely clear.

Disruptive technologies or scientific discoveries that are expected to have a major, or perhaps revolutionary, effect on NATO defence, security or enterprise functions in the period 2020 – 2040.

Convergent: A combination of technologies that are combined in a novel manner to create a disruptive effect.

The incorporation of Artificial Intelligence (AI) into the design of traditional battle networks is expected to enhance the performance of the current platforms of the armed forces around the world [20]. The massive investments made by countries like China, Israel, Russia and the United States in next generation defence systems and the large scale procurement of such systems by countries, like India, Japan, Saudi Arabia, and South Korea are expected to drive the growth of artificial intelligence and robotics in the aerospace and defence market.

The possibilities of influencing the three landscapes of the operating environment (Human; Physical; Information, see Figure 17-2) are much wider than the traditional military means. They include for instance interventions through social media, stratcom, cyber, and through cooperation with financial and utilities providers. All these possible actions have consequences in all the landscapes and contribute in the different ways to the desired effects. For a commander to effectively orchestrate actions in three landscapes, he needs support on possible courses of action, their effects and consequences. AI, simulation and traditional algorithms are techniques that can provide this functionality.

In the frame of combat systems, the Command and Control System (C2) allows the Commander and their team to manage in near-real time [21]:

a) System electronics;

b) Sensors;

c) Electronic warfare; and

d) Effectors, in order to generate Situational Awareness (SA) and ensure the tactical control of the area-of-operations.

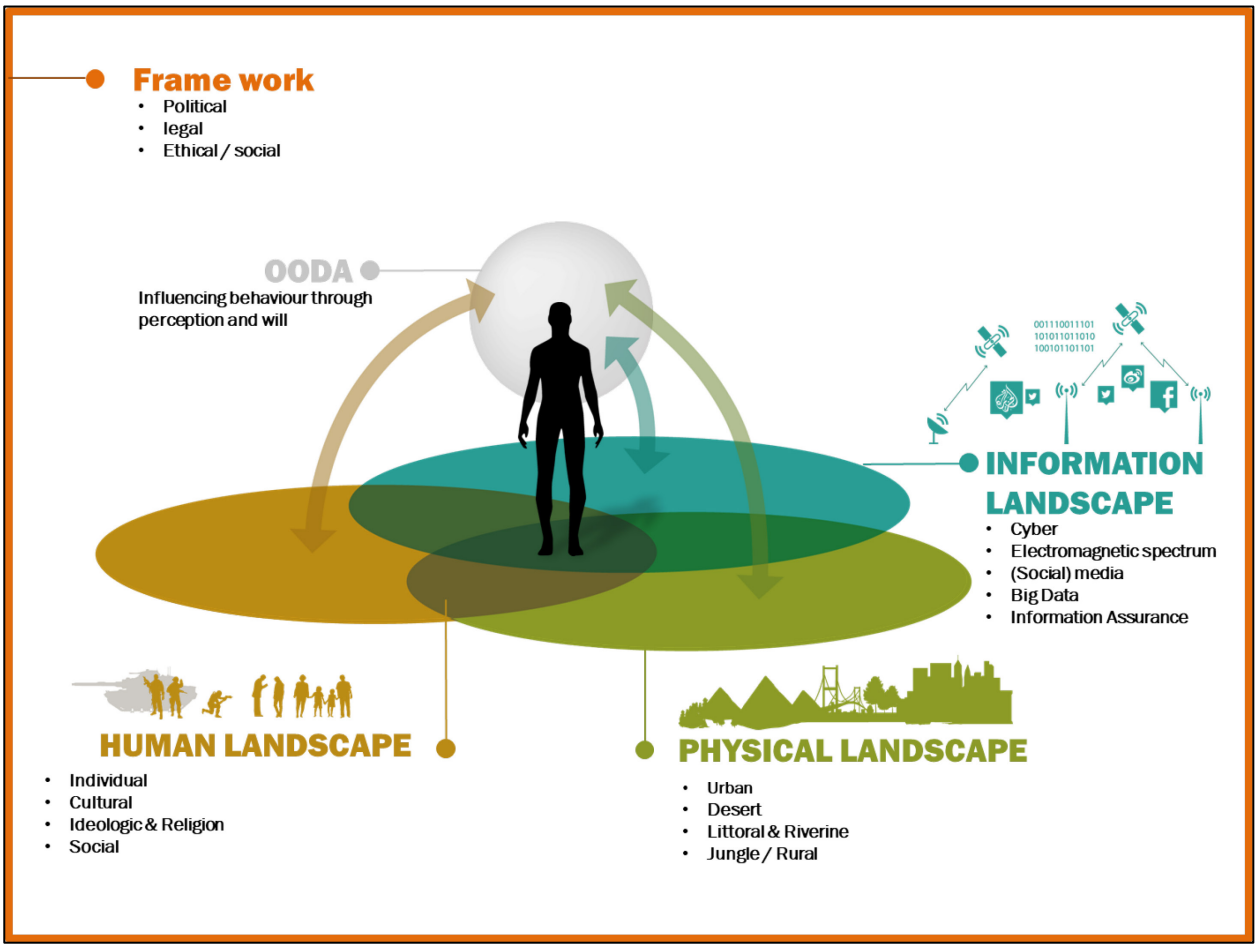

Figure 17-2: Possible Picture of Future C2-Support System.

Some of the major applications of AI systems in defence mechanisms are explained below in detail:

1) Warfare Platforms and Weaponry

Defence forces from different countries across the globe are embedding AI into weapons and other systems used on land, naval, airborne, and space platforms. Using AI in systems based on these platforms has enabled the development of efficient warfare systems, which are less reliant on human input [1]. It has also led to increased synergy and enhanced performance of warfare systems while requiring less maintenance. AI is also expected to empower autonomous and high-speed weapons to carry out collaborative attacks.

2) Cybersecurity

Military systems are often vulnerable to cyber-attacks, which can lead to loss of classified military information and damage to military systems. However, systems equipped with AI can autonomously protect networks, computers, programs, and data from any kind of unauthorised access. In addition, AI-enabled web security systems can record the pattern of cyber-attacks and develop counter-attack tools to tackle them. In defence circles, cyberspace is now being considered as the third war-front after land, sea, and air. A compromised and malicious network can severely compromise the security of the whole region. Defence establishments are using machine learning to predict and protect from unauthorised intrusions. This intrusion detection is usually done by classifying the network as normal or intrusive. AI-based techniques help in increasing the accuracy of such classification.

We found that AI solutions for cybersecurity have a high degree of demand. This seems understandable for cybersecurity due to the high level of risk associated with the data breaches in military and defence networks. Several AI vendors and defence contractors seem to be using machine learning to offer security products that can identify and predict threats before they can affect the networks. Cybersecurity threats come in numerous shapes and sizes. Artificial intelligence has the capability to play a large role in preventative measures for a military. Today, software is able to identify various digital situations, such as an email or a new flash drive, likely to be a trap or tool for implanting malware, and then neutralise the cyber threat lying in wait for a military operator before the malware can active.

3) Logistics and Transportation

One of the most important factors that play a role in determining the success of a military operation is logistics. Integration of machine learning and geospatial analysis with the military's logistical systems reduce the amount of effort, time, and error [22].

AI is expected to play a crucial role in military logistics and transport. The effective transportation of goods, ammunition, armaments, and troops is an essential component of successful military operations. Integrating AI with military transportation can lower transportation costs and reduce human operational efforts. It also enables military fleets to easily detect anomalies and quickly predict component failures. Recently, the US Army collaborated with IBM to use its Watson artificial intelligence platform to help pre-identify maintenance problems in Stryker combat vehicles.

An AI-powered transportation system is essential to transport weapons, food, troops, goods, and equipment in time and good condition. Machine Learning, Geospatial analysis, and their integration with the military's logistical systems reduce human effort, minimise costs, reduce errors, and detect anomalies faster.

AI may have future utility in the field of military logistics. The Air Force, for example, is beginning to use AI for predictive aircraft maintenance. Instead of making repairs when an aircraft breaks or in accordance with standardised fleet-wide maintenance schedules, the Air Force is testing an AI-enabled approach that tailors maintenance schedules to the needs of individual aircraft [22].

4) Target Recognition

AI techniques are being developed to enhance the accuracy of target recognition in complex combat environments. These techniques allow defence forces to gain an in-depth understanding of potential operation areas by analysing reports, documents, news feeds, and other forms of unstructured information. Additionally, AI in target recognition systems improves the ability of these systems to identify the position of their targets. Capabilities of AI-enabled target recognition systems include probability-based forecasts of enemy behaviour, aggregation of weather and environmental conditions, anticipation and flagging of potential supply line bottlenecks or vulnerabilities, assessments of mission approaches, and suggested mitigation strategies. Machine learning is also used to learn, track, and discover targets from the data obtained.

5) Battlefield Healthcare

In war zones, AI can be integrated with Robotic Surgical Systems (RSS) and Robotic Ground Platforms (RGPs) to provide remote surgical support and evacuation activities. The US in particular is involved in the development of RSS, RGPs, and various other systems for battlefield healthcare. Under difficult conditions, systems equipped with AI can mine soldiers' medical records and assist in complex diagnosis.

Medical backup is very crucial for the nation's defence. We all know that it is very difficult to provide medical support on the battlefield. For this reason, many countries are developing prototypes that are fully AI controlled medical assistants to provide medical support for the soldiers. These AI assistants are fully equipped with the medical history of the soldiers that help them to cross-reference the present

data with the previous information to provide the most effective diagnosis and take the measures accordingly. This ensures faster recovery of the soldier, better remedial support, and reduced human risk. AI operated machines can also be used to provide security and medical support while an evacuation process is underway. It ensures more enhanced security.

6) Combat Simulation and Training

Training and preparing the army personnel for wars and attacks is essential. The military uses AI and Machine Learning powered Augmented Reality (AR) and Virtual Reality (VR) as they create effective simulations that are realistic, dynamic, and adaptive. The reinforcement learning technique enhances the combat training for virtual agents and human soldiers.

Simulation and training is a multidisciplinary field that pairs system engineering, software engineering, and computer science to construct computerised models that acquaint soldiers with the various combat systems deployed during military operations. The US is investing increasingly in the simulation and training applications.

7) Threat Monitoring and Situational Awareness

Threat monitoring and situational awareness rely heavily on Intelligence, Surveillance, and Reconnaissance (ISR) operations. ISR operations are used to acquire and process information to support a range of military activities. Unmanned systems used to carry out ISR missions can either be remotely operated or sent on a pre-defined route. Equipping these systems with AI assists defence personnel in threat monitoring, thereby enhancing their situational awareness. Unmanned Aerial Vehicles (UAVs) – also known as drones – with integrated AI can patrol border areas, identify potential threats, and transmit information about these threats to response teams. Using UAVs can thus strengthen the security of military bases, as well as increase the safety and efficacy of military personnel in battle or at remote locations.

8) AI and Data Information Processing

AI is particularly useful for quickly and efficiently processing large volumes of data in order to obtain valuable information. AI can assist in culling and aggregating information from different datasets, as well as acquire and sum supersets of information from various sources. This advanced analysis enables military personnel to then recognise patterns and derive correlations.

17.2.2 Intelligence and AI

In the military context, the opportunities for remote-sensing, situational-awareness, battlefield-manoeuvre, and other AI applications seem promising. It remains unclear, however, whether these new technical capabilities will ultimately shift the balance in favour of offensive or defensive actions. Improved performance is one of the benefits that the interviewees had in mind when they discussed the use of big data. Additionally, however, they pointed out that the sheer volume of information being collected by various sensors is more than a human or team of humans can analyse. Given the ever-growing volume of data available in the world today, AI is expected to continue to increase in prominence.

Use of Big Data and Big Data Analytics

There are two trends in Data and Big Data Analytic first trend is centralised information processing and analytic. It allows using advanced methods and computing capability. Second trend is edge computing when selected algorithms are used directly on sensors (e.g., automatic number plate recognition or object/event detection on cameras) in order to provide higher value and at the same time to reduce amount of data, which need to be transferred. Edge computing can be realised also on desktop workstations – using data analytics techniques on local data sets.

According to a study by the EMC Corporation, the amount of data stored on Earth doubles every two years, meaning that as much data will be created over the next 24 months as over the entire prior history of humanity (Ref. [2], p. 55). Most of this new data is unstructured sensor or text data and stored across unintegrated databases. For intelligence agencies, this creates both an opportunity and a challenge: there is more data to analyse and draw useful conclusions from but finding the needle in so much hay is tougher. Modern intelligence agencies each day collect more raw intelligence data than their entire workforce could effectively analyse in their combined lifetimes (Ref. [2], p. 56).

Collection of Data

Militaries around the world acquire enormous amounts of visual surveillance data a day from various sources, such as phone cameras, laptop feeds, video surveillance, planted cameras, UAVs and satellite footage. The challenge is not collecting the data, but processing it for strategic information, and this is where machine vision and AI could be of use. Machine vision software has the potential to sort through large sums of data for insights faster than trained human analysts. We can infer from material stated by Google and the US Department of Defense the machine learning model behind the software used in Project Maven was trained to identify 38 different kinds of objects and so the AI was shown those individual objects across hours of footage from various angles and in various lighting conditions.

The objects within the footage would have been labelled as what we know the objects to be, such as a travelling car, a weapon, or a person. This labelled footage would then be run through the software's machine learning algorithm. This would have trained the algorithm to discern the sequences and patterns of 1s and 0s that, to the human eye, form the video of a combat zone as displayed in drone surveillance footage. The Pentagon has not publicly defined these 38 objects the software flags. The algorithm behind the software would then be able to determine the contents of the footage and identify any anomalies or relevant objects it has been trained to flag. The system then alerts a human operator in some unknown fashion and highlights the flagged objects within the video display.

Satellite imaging allows operators to track target movement over large areas, determine normal patterns of activity for a location, and detect anomalies when those patterns differ. Orbital Insights links together a large amount of satellite imaging data from various networks to assemble high definition images of any location on the globe, taking the most useful pieces of each while removing clouds, smog, weather effects, or haze from the images.

In the case of autonomous drones, many of them utilise GPS technology and tracking to allow operators to plot the general path of the drone's flight. As the drone is operating autonomously, the exact flight pattern and manoeuvres would be left to the artificial intelligence.

Processing of Information

As mentioned earlier, the biggest advantage of AI is that it can effectively analyse a large amount of data in significantly less amount of time and provide us the required results. This is the main reason behind incorporating AI in various fields, especially in defence. The data obtained from AI surveillance and reconnaissance is used to produce various threat patterns, formulate different strategies as well as the plans to tackle. Often these datasets can reveal various enemy patterns that are not visible to the naked eye. Thus, it can give an edge over the enemies so that we can make necessary arrangements to strengthen the nation's defence systems.

The AI systems can process a large amount of data in a comparatively shorter time as compared to normal strategists so that we can make up the valuable time loss by using artificial intelligence. Since we can formulate better strategies with the help of AI, it helps us to prevent valuable resources and life losses. With the advent of the digital age and increased use of data in almost every field, the need for upgrading the

defence systems is now higher than ever. To keep up with the rapid advancement of technology and the evolution of the threats, we face every day that AI is the only way to effectively strengthen the defence mechanisms and provide better security.

Intelligence Analysis and Big Data

Computer-assisted intelligence analysis, leveraging machine learning, will soon deliver remarkable capabilities, such as photographing and analysing the entire Earth's surface every day. Analysts must prioritise and triage which collected information to analyse, and they leverage computer search and databases to increase the amount of information that they can manage. Some datasets that could previously only be analysed by human staff, such as photos, are newly amenable to automated analysis based on machine learning. Since machine learning is useful in processing most types of unstructured sensor data, applications will likely extend to most types of sensor-based intelligence, such as Signals Intelligence (SIGINT) and Electronic Intelligence (ELINT). Machine learning-based analysis is also useful for analysing and deriving meaning from unstructured text.

AI with geospatial analysis can help in the extraction of valuable intelligence from connected pieces of equipment such as radars and automatic identification systems. This information can help in detection of any illegal or suspicious activities and alert the concerned authority. Robots with AI and computer vision with IoT can also help in target identification and classification.

One core capability of artificial intelligence is identifying trends and patterns within a data set to then predict the likelihood of, and when, that trend will occur again. This is called predictive analytics, and it is currently being applied to matters of homeland security. Predictive analytics models can be used to correlate signs of preparation for unlawful activities, such as purchasing a weapon or makeshift bomb-making material at a store, which allows intelligence agencies to intercept the act before a plot unfolds. Predictive analytics software can also give a prediction of possible suspects of a crime based on various environmental factors and past criminal record data. Pooling vast sums of data allows for the AI to find patterns correlative to unlawful action that data analysts may struggle to investigate and identify on their own.

Support to Decision Making

Driven largely by the progress observed in gaming systems and personal assistant technology,AI is anticipated to be able to recommend options to decision-makers more quickly, or in some cases, to be able to provide superior options to select from than humans could offer. A familiar example is routing technology that can ingest complete maps and real-time or projected traffic information in ways that humans would not be able to. There are natural applications of such capabilities in logistics, and they are also expected to help with other common tasks, such as scheduling.

The most frequently mentioned category of benefits of AI in warfare is speed. Interviewees often discussed this in reference to the OODA loop, with the idea being that if it is possible to cycle through the OODA loop faster than one's adversaries, then they will be unable to perform the counteractions needed to defend against attacks or to generate their own offensive options fast enough to outpace counteractions. There are certainly cases where this type of advantage can be envisioned; however, it is also important to keep in mind that timelines are not always dominated by the decision processes thatAI can help accelerate. Often the timelines are dominated by the time it takes to move equipment or people or even just the time that munitions are moving to targets. It is important not to overstate the value of accelerating the decision process in these cases.

Situational Awareness (SA) and Understanding (A2A)

The main application of military imaging systems is situational awareness: knowing who and what is in the vicinity and gaining an understanding of their behaviour. Image analysis techniques support the key tasks

that enable situational awareness: detection, tracking, classification, identification, and behaviour recognition of targets or objects, while avoiding too many false alarms or missed detections. Artificial Intelligence and Machine Learning are increasingly used to assist in these tasks, as the amount of sensor data increases while there are fewer analysts and camera operators available.

Drones are already taking hold in the defence environment. Efficiency savings can be made by making use of equipment, which is cheaper, more versatile and doesn't involve sending soldiers onto the frontline. This equipment was remote controlled, but AI can take drone technology to the next level, helping drones navigate and make sense of the world they operate in. Couple this with image recognition technology and there is potential for serious improvements in efficiency and mission success. However, with image recognition the drones themselves can provide detailed contextual analysis in real-time, leaving mission control to concentrate on strategy. Far from being a future consideration, this is already being explored in transport and civil infrastructure, using Neural Networks to detect and classify objects in coastline observation, fire detection, and three-dimensional mapping [24].

An appropriately organised data asset, with established procedures for continuous up-dates and a general mechanism to answer complex questions ad hoc would allow real-time (or at least near-real time), flexible responses to questions arising. This can include automated machine-to-machine communication for situational awareness on board of vessels, airplanes, drones, or any other mobile system requiring quick fusion of continuously updated data maintained at different sites – in short: federations. Of course, appropriate security is indispensable for such communication, posing particular challenges as potentially untrusted and trusted information needs to be processed for delivery to requestors of varying clearance.

Since military need to operate in the physical, human, and information landscapes, they need SA in all three landscapes (Figure 17-3). This includes insight in the context of the mission, the interaction between the landscapes, the role of actors in these landscapes and how they influence their environment. For better cooperation with partners,insight in their status, the progress of their actions and consequences of deviations can provide means for coordinated effects. Finally, all of these require a geographical representation and visualisation in order to connect to the human interpretation. Of course, there are multiple other information flows that can be of individual or situational dependent importance. This means that a future C2-support systems also needs possibilities for personalisation. AI can help to provide the military with the information that is tailored to their needs and current (cognitive) capabilities.

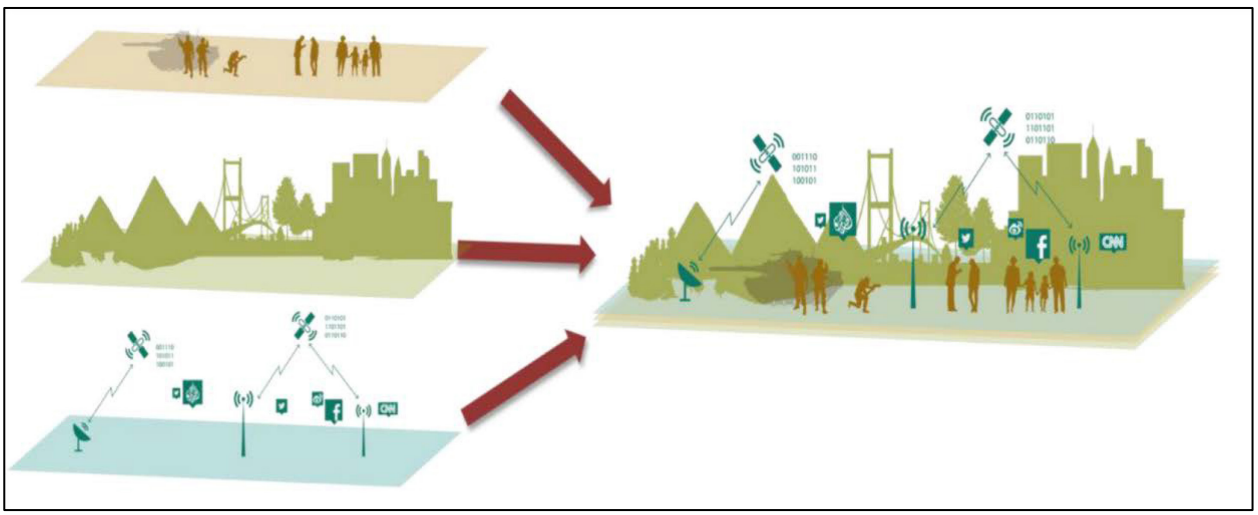

Figure 17-3: Three Landscapes Form the Operating Environment.

In order to orchestrate operations in these landscapes, military need Situational Awareness (SA), insight in the possible Courses of Action (CoA) and their effects in all three landscapes of themselves, their partners and (where possible) their adversaries. Present C2-support systems mainly provide SA in the physical domain and some decision support. The human and information landscapes are not or barely covered and insight on the interaction between the three is not available at all. Big data and AI can be used to support military decision making in a wide range of circumstances at the strategic, tactical or operational levels, and in support of all military capabilities in all landscapes. In order to restrict the range of applications, we propose to limit them to two capabilities that are operationally relevant and that generally involve complex, time-critical decisions [25]:

- Situational Awareness, and
- Command and Control.

While greatly supporting force projection in asymmetric conflicts, UAVs at present still know a number of operational limitations, such as a low flying speed and vulnerability to air defence systems. Increasing the autonomy of unmanned systems will strengthen their survivability, enable more higher-end performance, and improve their effectiveness at patrolling or monitoring areas. This feeds into an increased ability for militaries or states to cover far greater areas with sensors, at greater cost-effectiveness than human troops. The enhanced situational awareness enabled by more autonomous and survivable drones can strengthen the security of bases and, experts have suggested, could potentially lead to greater stability between states (such as North and South Korea) by enhancing monitoring of contested areas, reducing the viability of covert or 'hybrid' operations [26].

17.3 HUMAN ENHANCEMENT

17.3.1 Bio Technologies and Human Enhancement

Bio and Human Enhancement Technologies (BHET) are expected to be available over the next 20 years that will change the very definition of what it means to be a soldier, sailor, aviator, or spaceman. Exploitation of bio and human enhancement technologies can provide new health and medical remedies to enhance the human level of resiliency by using biotechnological medicine as a countermeasure, especially against new emerging biological threats (for example a pandemic), while biosensors and biometric collection will support a more comprehensive understanding of the human and mission environment. As with the aforementioned EDTs, China is investing heavily in 'life sciences' R&D and external assessments judge that China has transitioned from a 'me too' position to one of being a true innovator. In its national strategy of 'military-civil fusion', China has prioritised biology as a new domain of warfare and biotechnology is intended to become the new 'strategic commanding heights' of China's national defence. The COVID-19 pandemic has vividly demonstrated how a virus can severely impact human activity on a global scale and reinforces the need for Alliance forces to be prepared and equipped to maintain an effective operational posture in the most hostile of biological environments.

Biotechnology has become an increasingly agile platform for developing new types of soldier enhancements (Figure 17-4). As such, the field offers novel opportunities for improving war fighter survivability on the battlefield.

Modern biotechnology could be used directly as a means of defence and attack, and with further development, they will become new weapons and their capability of attacking targets accurately.

Biological cross-technology, drawing on and using the many excellent structures and special functional principles of biology, will provide a new source to accelerate the development of weapons and equipment. For example: The application of high-performance bionics and biomaterials could provide a new material

basis for weapons and equipment. Biosensing technology, based on the specific identification of biomolecules, has the advantages of ultra-high sensitivity and difficulty in interference and will change the means and capabilities of battlefield situation awareness. Computing technology will break through the physical limits of traditional computer space, heat dissipation and parallelism, triggering a revolution in military computers.

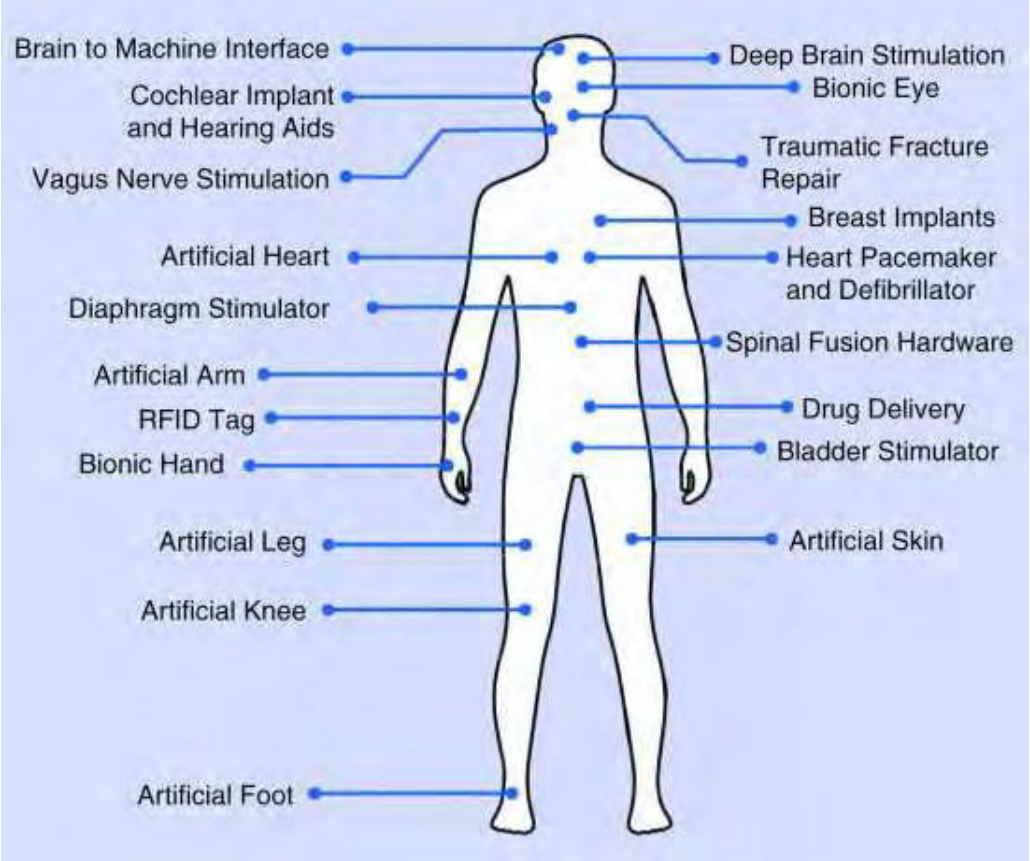

Figure 17-4: Typical Artificial Implants.

Human augmentation refers to technologies that enhance human productivity or capability, or that somehow add to the human body or mind. Three main categories of enhancement:

- Enhanced senses, extended senses, achieved by interpreting available multisensory information and presenting content to the human through selected human senses. Sub-classes include augmented vision, hearing, haptic sensation, smell, and taste.
- Enhanced cognition is achieved by detecting human cognitive state, using analytical tools to make a correct interpretation of it, and adapting computer's response to match the current and predictive needs of the user (e.g., providing stored or recorded information during natural interaction).
- Augmented action, achieved by sensing human actions and mapping them to actions in local, remote or virtual environments. Sub-classes include motor augmentation, amplified force, and movement, speech input, gaze-based controls, teleoperation, remote presence, and others.

There are different ways to deliver Human Enhancement Technologies (HET): cognitive, physical, sensory:

- Cognitive enhancements are interventions that improve cognitive abilities. Potential targets for cognitive enhancement are intelligence, clarity and creativity.

- Physical enhancements are interventions that improve or introduce new physical abilities. Potential targets for physical enhancement are performance, endurance, or the addition of new abilities (additive). Performance enhancements increase the capacity to complete physically demanding tasks, like running quickly or lifting heavy objects. Endurance enhancements increase the capacity to engage in physically demanding tasks for extended periods.
- Sensory Human-Machine Interface (HMI) systems have emerged from medical therapeutics for visual and hearing loss. Visual capability can be modified using non-invasive approaches such as eyewear (e.g., goggles, contact lenses), and/or invasive instrumentation for modification of retinal network sensitivity, direct input to the optic nerve and or tract, and indwelling hardware to enable remote open-, semi-closed- and contained closed-loop modulation of visual cortical function (i.e., "eyeless vision"). Similarly, auditory HMI systems can be non-invasive (e.g., earphones, earbuds), and/or invasive as based upon extant cochlear and spiral ganglion implant technologies that – when used individually or in concert – can afford expanded (viz. subsonic/ultrasonic) auditory capabilities via direct interface with cranial neural components. In addition, external body coverings are being developed that afford enhanced tactile inputs and sensitivities. Overviews and additional detail of these developments are provided in the open-source academic and governmental literature.

17.3.1.1 Exoskeletons

Exoskeletons were meant to assist soldiers in a bunch of support tasks, including loading supplies, getting missiles onto airplanes, and repairing ships (Figure 17-5). In general, military exoskeletons in developed countries are moving out of laboratories to the battlefield. China has joined the exoskeleton Arms Race initially launched between US and Russia. In October 2019, PLA Army equipment department held a competition for the best exoskeleton designs. The contest featured fifty prototypes fielded by twenty-nine teams.

Figure 17-5: Status Quo of Active Exoskeleton.

The pipeline of biotechnology products likely to emerge over the next decade probably will result in disruptive innovations and significant societal impacts. Currently biotechnology seems to be underestimated in its exploitation in military applications with the respect, as a main example, to soldier resilience and survivability. NATO Science & Technology Organisation has been addressing the Biotechnology and the Human Enhancement since the early 2000s with a number of studies related to the enhanced capability of soldiers both from cognitive and physical points of view, and on exploitation of virtual and augmented reality. More recently specific topics related to biotechnology, such as synthetic biology, have been taken into consideration.

17.3.2 Defence Sector and AI/BHET

If one country fields machines that autonomously target and kill humans, it could be quickly followed by others, resulting in destabilising global arms races.

The Convention on Certain Conventional Weapons (CCW) at the UN has concluded a few rounds of meetings on lethal autonomous weapons systems in Geneva, under the auspices of what is known as a Group of Governmental Experts. Both the urgency and significance of the discussions in that forum have been heightened by the rising concerns over Artificial Intelligence (AI) arms races and the increasing use of digital technologies to subvert democratic processes [27]. Moreover, the discussions taking place at the UN are focused on autonomy in weapons, which is only partially related to larger issues of an AI arms race – although establishing norms on the automated control of conventional weapons, such as meaningful human control, could certainly advance discussion in other areas, such as cyberwarfare and AI ethics. Positive and meaningful action on this issue is still within reach, and it is up to the diplomats at the Convention on Certain Conventional Weapons and their governments to prove that they can work together to address the full range of threats to humanity posed by autonomous weapons.

The international regulation of autonomous weapons is an emerging issue for international law [28]. Many experts warn that lethal autonomous weapons would violate fundamental legal and ethical principles and would be a destabilising threat to international peace and security. Moral and ethical concerns have centred around the delegation of the kill decision to an algorithm. Legal concerns are related to whether lethal autonomous weapons could comply with International Humanitarian Law (IHL, also known as the law of war), more specifically whether they could properly distinguish between civilians and combatants and make proportionality assessments. Military and legal scholars have pointed out an accountability vacuum regarding who would be held responsible in the case of an unlawful act [29], [30]. Others have voiced concerns that lethal autonomous weapons would be seriously destabilising and threaten international peace and security. For example, by enabling risk-free and untraceable attacks they could lower the threshold to war and weaken norms regulating the use of force.

There are concrete steps companies can take to prevent their products contributing to the development and production of lethal autonomous weapons:

- Commit publicly to not contribute to the development of lethal autonomous weapons [31].
- Establish a clear policy stating that the company will not contribute to the development or production of lethal autonomous weapon systems. This policy should include implementation measures such as:
  - Ensuring each new project is assessed by an ethics committee;
  - Assessing all technology the company develops and its potential uses and implications;
  - Adding a clause in contracts, especially in collaborations with ministries of defence and arms producers, stating that the technology developed may not be used in lethal autonomous weapon systems.
  - Ensure employees are well-informed about what they work on and allow open discussions on any related concerns.

The low-cost of cyber has given offence the edge for targeted digital attacks. Widespread availability of low-cost, highly-capable, lethal, and autonomous robots could make targeted assassination more widespread and more difficult to attribute. A small, autonomous robot could infiltrate a target's home, inject the target with a lethal dose of poison, and leave undetected. Alternatively, automatic sniping robots could assassinate targets from afar.

However, the application of AI in war raises new and complex ethical questions regarding its role vis-à-vis the role of human war fighters. Such questions include whether AI systems can comply with humanitarian principles, whether they will be sufficiently reliable and predictable, and what effects they will have on escalation and stability.

Table 17-2: Companies and Projects [31].

COMPANY	BEST PRACTICE	MEDIUM CONCERN	HIGH CONCERN	HQ	RELEVANT TECHNOLOGY	RELEVANT MILITARY/ SECURITY PROJECTS	COMMIT TO NOT DEVELOP
AerialX			■	Canada	Counter-drone systems	DroneBullet	
Airobotics		■		Israel	Autonomous drones	Border security patrol bots	
Airspace Systems			■	US	Counter-drone systems	Airspace interceptor	
Alibaba		■		China	AI chips, Facial recognition	-	
Amazon			■	US	Cloud, Drones, Facial and speech recognition	JEDI, Rekognition	
Anduril Industries			■	US	AI platforms	Project Maven, Lattice	
Animal Dynamics	■			UK	Autonomous drones	Skeeter	X
Apple		■		US	Computers, Facial and speech recognition	-	
Arbe robotics	■			Israel	Autonomous vehicles	-	X
ATOS		■		France	AI architecture, cyber security, data management	-	
Baidu		■		China	Deep learning, Pattern recognition	-	
Blue Bear Systems			■	UK	Unmanned maritime and aerial systems	Project Mosquito/LANCA	
Cambricon		■		China	AI chips	-	
Citadel Defense			■	US	Counter-drone systems	Titan	
Clarifai			■	US	Facial recognition	Project Maven	
Cloudwalk Technology		■		China	Facial recognition	-	
Corenova Technologies			■	US	Autonomous swarming systems	HiveDefense, OFFSET	
DeepGlint		■		China	Facial recognition	-	
Dibotics		■		France	Autonomous navigation, Drones	'Generate'	
EarthCube			■	France	Machine learning	'algorithmic warfare tools of the future'	
Facebook		■		US	Social media, Pattern recognition, Virtual Reality	-	
General Robotics	■			Israel	Ground robots	Dogo	X
Google	■			US	AI architecture, Social media, Facial recognition	-	X
Heron Systems			■	US	AI software, ML, Drone applications	'solutions to support tomorrow's military aircraft'	

Artificial Intelligence (AI) has the potential to make many positive contributions to society. But in order to realise its potential, it is important to avoid the negative effects and backlashes from inappropriate use of AI. The use of AI by militaries in itself is not necessarily problematic, for example when used for autonomous take-off and landing, navigation or refuelling. However, the use of AI to allow weapon systems to autonomously select and attack targets is highly controversial. The development of these weapons would have an enormous effect on the way war is conducted. It has been called the third revolution in warfare, after gunpowder and the atomic bomb. Many experts warn that these weapons would violate fundamental legal and ethical principles and would destabilise international peace and security. In particular, delegating the decision over life and death to a machine is seen as deeply unethical.

17.4 ETHICAL ISSUES AND CONCLUSIONS

17.4.1 Ethical Issues

The use of AI in defence also presents an ethical dilemma. Experts and organisations around the world have raised such technology unintentionally escalating the tensions between countries. One of the arguments is that if an AI system fails to perform as intended may result in catastrophic implications. In fact, several human and civil rights groups call for an absolute ban on autonomous devices in defence, especially weaponry.

If machines that autonomously target and kill humans are fielded by one country, it could be quickly followed by others, resulting in destabilising global arms races.

17.4.2 Conclusions

Human interaction with Artificial Intelligence (AI) and AI's role in military systems is a very important consideration for defence policy makers in the near future. A level of human control has to be considered at the very first place in design and operation of systems with autonomous capability. In the military context, it is important that AI systems remain under appropriate human control. Nations are tackling different strategies towards the role of the human operator and the role of the machine in systems that use AI. Some nations aim at low level of independence with strong human involvement while other nations may tend to higher level of independence, ensuring more automated commandment. China has clearly demonstrated a preference for the adoption of AI with a high level of automation while the US or Europe have shown more resilience.

The rate of advance in technology has reached an inflection point. The pace of change for Artificial Intelligence and BHET is advancing much faster than experts had predicted. These advances will bring profound benefits to humanity as these systems help tackle tough problems in medicine, the environment, and many other areas. However, this progress also entails risks. Advances will enable new, disruptive innovations for military power. AI has the potential to enable many new types of low-cost, high-impact military technologies. Some of these may make nations' current investments unattractive.

Recommendations for nations:

- Review present technology exchange processes and programmes to reduce the risk of technological/industrial espionage.
- Develop guidance regarding technology transfer and of the security risks associated with outward overseas investments and inward Foreign Direct Investments (FDI).
- Introduce a process to evaluate emerging technologies to determine their technical viability, potential for adoption, the industry relevance across more than one sector, the likely speed of take-up and the level of public/private investment.

- Collaborate with a NATO body or agency for the development and management of a knowledge database and to maintain a strategic oversight of the relevant technology R&D programmes.
- Improve the engagement between nation and Small and Medium Enterprises (SMEs) to enhance their contributions to the innovation process.
- Continue to promote the creation of Centres of Excellence (CoE) for fostering the knowledge area development.
- Introduce a requirement that academic collaboration and research exchanges are to comply with the conditions in a framework agreement and not be stand-alone initiatives.
- Encourage to academic institutions to engage in technological projects in the area of ETs in coordination with national authorities.
- Organise, train, and equip forces to prevail in a world in which military systems empowered by ETs are prominent in all domains.
- Understand how to address the ethical concerns expressed by technologists, the private sector, and the national public.
- Commit to mitigating ethical risks associated with ETS such as "killer robots".
- Seek greater technical cooperation and policy alignment with allies and partners regarding the development and employment of military ETs.

17.5 REFERENCES

[1] Singh, T. and Gulhane, A. (October 3, 2018), "8 key Military Applications for Artificial Intelligence in 2018, market search", 8 Key Military Applications for Artificial Intelligence in 2018 (marketresearch.com) Retrieved 7 March 2017.

[2] NATO Industrial Advisory Group (NIAG) (08 January 2021), NIAG Study order for study group 252, "Emerging and disruptive technology in the context of emerging powers", Final Study Report, AC/259-D(2021)0001, NIAG-D(2021)0004 Retrieved 12 April 2021.

[3] Horowitz, M.C. (23 April 2018), "The promise and peril of military applications of artificial intelligence", Stanley Center For Peace and Security.

[4] Vincent, J. (4 September 2017), "Putin says the nation that leads in AI 'will be the ruler of the world'", The Verge. Putin says the nation that leads in AI 'will be the ruler of the world' - The Verge Retrieved 4 August 2018.

[5] Kumar, V. (February 11, 2021), "How AI startups are disrupting the defence and security industry?" Analytic Insight, A Look at 5 AI Startups Empowering Defence and Security Industry (analyticsinsight.net) Retrieved 12 September 2021.

[6] Sayler, K.M. (November 10, 2020), "Artificial Intelligence and National Security, Congressional Research Service.

[7] China State Council (July 20, 2017), "A next generation artificial intelligence development plan", trans. New America, https://rwww.newamerica.org/documents/1959/translation-fulltext-8.1.17.pdf Retrieved 22 December 2018.

[8] Horowitz, M.C. (May 2018), "Artificial intelligence, international competition, and the balance of power", Texas National Security Review 1, no. 3, p.39.

[9] Webster, D.R. (1987), "An introduction to artificial intelligence", in A.M. Din (Ed.), SIPRI, Arms and Artificial Intelligence: Weapons and Arms Control Applications of Advanced Computing, Oxford University Press: Oxford, p. 33.

[10] Cummings, M.L. (January 2017), "Artificial intelligence and the future of warfare", Research Paper, Chatham House, International Security Department and US and the Americas Programme, Retrieved 4 May 2018.

[11] Hutchins, A.R., Cummings, M.L., Draper, M. and Hughes, T. (2015), "Representing autonomous systems' self-confidence through competency boundaries", paper presented at the 59th Annual Meeting of the Human Factors and Ergonomics Society, Los Angeles, CA, 26 – 30 October 2015.

[12] Bergstein, B. (15 December 2017), "The great AI paradox", MIT Technology Review, https://www.technologyreview.com/2017/12/15/146836/the-great-ai-paradox/ Retrieved June 1 2018.

[13] Tonin, M. (13 October 2019), "Artificial intelligence: Implications for NATO's armed forces", NATO Science and Technology Committee, NATO Parliamentary Assembly, p.9. https://www.nato-pa.int/download-file?filename=sites/default/files/2019-10/REPORT%20149%20STCTTS%2019%20E%20rev.%201%20fin-%20ARTIFICIAL%20INTELLIGENCE.pdf Retrieved 12 April 2020.

[14] Allen G. and Chan, T. (2017), "Artificial intelligence and national security", Belfer Center for Science and International Affairs, p. 24.

[15] Scharre, P. (29 February 2016), "Autonomous weapons and operational risk", CNAS.

[16] Singer, P.W. (2009), "Wired for war: The robotics revolution and conflict in the twenty-first century", New York: Penguin Press, p. 128.

[17] Maxwell, P. (April 20, 2020), "Artificial intelligence is the future of warfare (just not in the way you think)", Modern War Institute, Artificial Intelligence is the Future of Warfare (Just Not in the Way You Think) - Modern War Institute (usma.edu) Retrieved 12 July 2020.

[18] Albert, D.S. (2000), "Network centric warfare: Developing and leveraging information superiority", 2nd edition, DOD CCRP.

[19] Nagpal, K. "Artificial intelligence in defence sector", DefenceProAc, https://defproac.com/?p=7231 Retrieved 17 June 2020.

[20] Mordor Intelligence, "Artificial intelligence and robotics in aerospace and defense market – growth, trends, COVID-19 impact, and forecasts (2023 – 2028)", https://www.mordorintelligence.com/industry-reports/artificial-intelligence-market Retrieved 8 June 2020.

[21] Frisoni, D. (2020), "Potential impact of artificial intelligence to C2 systems", Joint Air & Space Power Conference 2020. https://www.japcc.org/potential-impact-of-artificial-intelligence-to-c2-systems/ Retrieved 8 September 2020.

[22] Goled, S. (01 November 2020), "What are the scope and challenges of using AI in military operations?", Analytics India Magazine.

[23] Gregg, A. (16 Dec 2020), "In a first, Air Force uses AI on military jet". https://www.washingtonpost.com/business/2020/12/16/air-force-artificial-intelligence/

[24] DEFSEC Media (Summer 2017/18), "AI and machine learning: A new kind of military intelligence", Line of Defence Magazine.

[25] De Spiegeleire, S., Maas, M., Sweijs, T. (2017), "Artificial intelligence and the future of defense: strategic implications for small-and medium force providers", The Hague Centre for Strategic Studies (HCSS).

[26] United States, Joint Chiefs of Staff (2010), "Foreign internal defense", Joint Publication, JP 3-22, Washington, D.C.: Joint Chiefs of Staff, http://purl.fdlp.gov/GPO/gpo29282 Retrieved 26 June 2017.

[27] Astro, P. (27 April 2018), "Why the world needs to regulate autonomous weapons, and soon", The Bulletin, (April 27, 2018). https://thebulletin.org/2018/04/why-the-world-needs-to-regulate-autonomous-weapons-and-soon/ Retrieved 13 June 2019.

[28] Bento, L. (2017). "No Mere Deodands: Human Responsibilities in the Use of Violent Intelligent Systems Under Public International Law", Harvard Scholarship Depository, https://dash.harvard.edu/handle/1/33813394 retrieved 18 October 2018

[29] Docherty, B. (9 April 2015), "Mind the gap: The lack of accountability for killer robots", Human Rights Watch, https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots

[30] Thomas Chengeta (30 September 2015), "Accountability gap, autonomous weapon systems and modes of responsibility in international law", SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755211 Retrieved 7 July 2017.

[31] Conn, A. (18 July 2018), "AI Companies, researchers, engineers, scientists, entrepreneurs, and others sign pledge promising not to develop lethal autonomous weapons", Future of Life Institute, https://futureoflife.org/2018/07/18/ai-companies-researchers-engineers-scientists-entrepreneurs-and-others-sign-pledge-promising-not-to-develop-lethal-autonomous-weapons/ Retrieved 21 March 2019.

Chapter 18 – FINDINGS, CONCLUSIONS AND TOPICS FOR FURTHER RESEARCH

Jaan Murumets
Estonian Military Academy
ESTONIA

This chapter brings together shortfalls and challenges identified in case studies, draws preliminary conclusions, and outlines sub-fields and topics to be further researched. Some of these topics are addressed in Phase 2 of the SAS-152 study with highlights of these chapters provided further below. Some of the topics, however, wait to become separate research projects outside of the scope of this study.

18.1 IDENTIFIED CHALLENGES

Collaboration across organisational boundaries has many challenges. Actors in implementing the concept of comprehensive defence are extremely diverse in terms of statutory goals, organisational structures, guiding doctrine (spelled-out as well as implicit) and working practices.

18.1.1 Belgium

The Belgian Defence is exposed to stakeholder complexity and the challenge this constitutes to further development of comprehensive approach. The case study of Belgium derived the factors that challenge implementation of the concept of comprehensive defence in two broad categories: structural (or hard), and conceptual (or soft) factors.

Challenges in the category of hard factors appear to boil down to adverse effects of highly complex and nuanced system of local and regional governments, with the federal government on top often based on unstable parliamentary coalition. This makes achieving and maintaining political unity beyond short term virtually impossible, which – in turn – complicates development of long-term vision and strategy. Further, the complexity of the government system raises constantly questions relating to sovereignty, control over resources, and control over decisions. The corollary to that is the difficulty of synchronising and harmonising decision making across stakeholders, particularly in the context of major equipment projects, often amplified by very different values and objectives of different organisations within a partnership.

The structural challenges outlined above are complemented by soft factors, one of the most notable of which is difference in perception of time: the defence sector adopts multiple planning horizons from next year to long-term visions twenty-thirty years down the road, whereas law enforcement and rescue sectors tend to focus on responding to crises in real time and near-future. Another challenge is that of meta-languages characteristic to different domains of activity, and terminology. For instance, the defence sector uses language full of abbreviations and specific terms which may not be understood outside the organisation. The problem is made worse as the two most widely spoken languages in Belgium – Dutch and French – often have different grammatical and vocabulary means to express the same concept. This creates confusion, arbitrary interpretation, and fatigue amongst stakeholders as to what is actually being discussed. Further, the difference in the structure of various partners often plays a role. Defence organisations are characterised by a well-developed hierarchy with clear decision-making responsibilities, whereas other governmental agencies tend to have a flatter structure and less sophisticated decision-making process. NGOs have an even more decentralised structure, little hierarchy and may be making decisions based on consensus. In general, many stakeholders lack knowledge about partner organisations (including their hierarchy and decision-making process) which contributes to a lack of trust and misconceptions. In order to be able to work well together

within a complex framework such as comprehensive defence, it is therefore important to overcome some of these structural differences, as well as those of organisational culture.

18.1.2 Estonia

The four main players in the crisis management system – the Defence Forces (including the Defence League), Police, Rescue Board and Health Board – have strong identities, traditions, and organisational culture. In building the cooperation between key stakeholders and conducting joint activities, the problem of the institutional barriers cannot be ignored. On one side, it is related to a habit to protect the valuable and sensitive information. On another, it copies the real world: all these agencies are also competitors for the resources. Defence sector aside, there are no clear strategies on funding and other agencies are facing problems to develop a long-term perspective in resource planning.

When responding to emergencies, all agencies use their own SOPs, based on their knowledge and departmental best practices. There is no common approach and standards in place that are accepted by everyone. Another challenge is the terminology. For every agency, the same terms may have the different meaning. For instance, the word “operation” has a completely different meaning in military and in police. In the established practice of multi-agency emergency response, ad hoc decision support structures (staffs) would be organised around the lead agency depending on the nature of the emergency with default SOPs being those of the lead agency. To minimise resulting friction, development of the common SOP is crucial.

18.1.3 Latvia

Latvia started to implement the CND system in 2018, thus, for now, only the first steps have been taken in these fundamental changes in the approach to national security. Challenges identified for Latvia are issues related to state and society relations and social cohesion. The analysis of the vulnerabilities of Latvian society revealed two significant problem areas in Latvian society, related to the ethnic structure and estrangement between society and the state: the majority of a population in Latvia distrusts parliament and government. The study discovered the more pronounced alienation of Latvia’s ethnic minorities from the state; in the context of CND system implementation, it poses a challenge to achieve a common vision on security issues in both language groups.

Latvia also experiences constant pressure from Russia in the media environment, and the implementation of the CND system is no exception. Concerning CND system implementation, Latvian government, and defence sector in particular, should focus not only on change management but also has to overcome destructive trends in the information environment.

18.1.4 Norway

Actors in the total defence, like everyone else in society, depend on a variety of societal functions and services, some of them critical to the performance of their duties. Over recent decades, the public sector has been reorganised and privatised, and businesses and infrastructures have become more international. The private sector has therefore increased its importance as a premise for national preparedness and the total defence: both are dependent on private-public cooperation and the secure supply of goods and services in an international framework. In the context of rapid technology development, it is yet uncertain how vulnerable the various critical societal functions are to disturbances, sabotage, and direct attacks. Understanding the weaknesses and vulnerabilities of the technologies and systems the Armed Forces and the Total Defence depend on is of crucial importance.

Another challenge relates to basic national functions that are partially or in full carried out by businesses that operate within a globalised network encompassing just in-time production and reduced stocks. The Security Act establishes specific requirements for critical goods and services – enforcing these requirements in a

compressed time-scale may prove problematic due to the complexity of the functions and supporting infrastructures. The modern digitalised society is critically dependent on electronic communications, electric power supply and satellite based services. Hence, maintaining a sufficient resilience of society's critical functions may become a challenge.

18.1.5 Turkey

Defence policy-making in Turkey does not receive enough input from civilian actors in the government, academia, or the civil society. The lack of expertise and accumulation of knowledge is the main reason why Turkey's defence policy is formulated by a very narrow circle within the state. Private actors such universities, research centres, corporations, banks, and civil society organisations are generally not connected to the security area due to the state centric system.

18.1.6 United Kingdom

Security professionals within government and Defence are able to articulate current threats which are most dangerous to the nation but national security, and those who contribute to it, are perhaps less well understood by the public. The British public's relatively poor perception of national security highlights the lack of engagement between the British government and the British people on matters of Defence policy. The apparent communication gap undermines the ability to effectively develop a coherent strategy for the use of military force and acts as a barrier to address how the military can better contribute to national defence in a domestic setting. Public buy-in and trust are essential components of creating a Comprehensive National Defence System; the most effective way for the UK model to adapt its current approach to domestic security and resilience is to widen the debate and seek greater public input.

The UK approach to national defence remains to 'defend away'. This represents a potential gap in doctrine where security and resilience are based almost exclusively on civil contingencies with the military in a limited supporting role and the primary focus of the military instrument concerned with deploying at reach. Modern threats are no longer clearly separated into neat categories of home and away and the distinction between war and peace is increasingly blurred. Although the UK approach to resilience and security has many strengths, it is debatable whether the current framework would be able to effectively respond to a cascade of threats or a complex challenge that absorbs more than just spare capacity from an already overstretched force.

Resilience and redundancy are key challenges for domestic security and to resource this is an imaginative and innovative way, a positive societal perception of the military must be a priority to move closer to a Comprehensive National Defence System.

18.2 PRELIMINARY CONCLUSIONS OF PHASE 1

18.2.1 Literature Review

As became evident from the review of literature, the top journals in the field (based on bibliometric results, as well as impact factor considerations) are the Journal of Humanitarian Logistics and Supply Chain Management, followed by International Peacekeeping, Small Wars and Insurgencies, and the Journal of Strategic Studies. In terms of authors, it appeared that 25 authors had two or more publications in the final paper set, out of which twelve authors seemed to focus on the topic only. Three clusters of authors were also identified which were all connected by at least one author. Further, the results also indicated that the U.S.A and the Netherlands are probably the countries which may be specifically invited to participate in future studies related to the comprehensive approach concept.

The literature review identified the main stakeholders of defence organisations as being Ministries (such as Foreign Affairs and International Aid), politicians (such as Heads of Government, Ministers, the Government, and Party leaders), national coordinating bodies (such as National Security Councils), International organisations (such as NATO and the EU), bilateral and multilateral partners, one's own society or population, the media, crisis management actors (such as the Police and Civil Protection), intelligence agencies, cyber agencies, humanitarian organisations (such as the ICRC) and private companies. Although the review did not identify a single comprehensive approach framework incorporating all these different stakeholders, it was possible to identify 3D (Defence, Diplomacy and Development) together with its variations – the Whole-of-Government approach, the Integrated approach, Total Defence, and the national crisis management systems – as the most prominent frameworks. While the Integrated approach seems to be the preferred form of collaboration in complex expeditionary operations, Total Defence appears to be the method of choice for defence of the homeland and resilience.

18.2.2 State of Development and Implementation of the Concept

Inter-agency cooperation in implementation of Comprehensive Defence concept can take place at different levels and to various degrees. It can be measured in how comprehensive the National Security Strategy or similar doctrinal documents of the country are; it can also be measured in the extent of joint (inter-agency) procurement, the level of cooperation between different organisations in real-life operations, and qualitative assessments during joint crisis management exercises.

When using some of these instruments to assess the state of comprehensive approach in **Belgium**, it can be characterised as emergent. The approach is limited to the 3D-LO concept geared towards external crises, it does not provide an answer to the nexus between internal and external safety and security, it does not provide for formal reporting mechanisms to the Federal Government, and does not in itself contain any specific objectives and goals. Inter-agency cooperation seems to occur when there is not much at stake, when the different actors are able to retain control of resources, and when national or organisational sovereignty is preserved. In the future, top-down vision, coordination, and directives appear necessary to make hard decisions and to extend the cooperation task specialisation in capability generation and deployment.

The **Estonian** comprehensive defence concept is relatively well-developed at the strategic level through the existing National Security Strategy and overarching medium- and long-term development plans. Estonia has also a solid practice of inter-agency cooperation in practical emergency response and conduct of joint exercises on different levels. The years of implementing the current security strategy and NDDP provided Estonia with lessons learned. There should be better harmony between broad security and comprehensive defence concepts and the legislation. The existing legal construct, based on three different laws (The Emergency Act, The State of Emergency Act and The National Defence Act) is too complex and doesn't ensure clarity and continuity in governance during the crises. The main emphasis should therefore be on clarification of the roles and responsibilities of different stakeholders on crisis management and simplification the crisis management system as a whole. To enhance the inter-agency cooperation, the crisis management system needs the standardised SOPs and solid doctrinal base, even though ad hoc solutions appear been working well.

CND system in **Latvia** is primarily a way of thinking because current activities are aimed at informing and educating the representatives of the responsible and involved institutions, as well as society in general. So far the focus had been on the more effective use of existing structures and resources. The three pillars of the CND mind-set are: resistance – in case of military attack Latvia will resist; responsibility – national security is a responsibility of every member of Latvian society; and cooperation – force structures, public administration institutions, municipalities, NGOs, commercial organisations, and individual members of society cooperate to protect Latvian statehood.

The **Norwegian** comprehensive defence system or whole-of-government approach to crisis management is denoted the "total defence concept". The concept means that all available actors and resources, military as well as civil, should cooperate to prevent, prepare, handle and recover from crises. The Government has the overall executive responsibility for state security, societal security and emergency prevention, preparedness planning and crisis management. Norway bases her societal security, emergency preparedness and crisis management on four fundamental principles: responsibility, similarity, proximity, and cooperation. In addition to these fundamental principles, Norway emphasises civil-military cooperation to manage severe crises. The overall objective is a balanced approach to civil-military cooperation within the total defence framework encompassing both civil support to the Armed Forces in crises and armed conflict, as well as military support to civil crisis management in peacetime. Armed Forces' operational capability inherently rests on civil support and civil infrastructures and services.

Turkey has a well-working crisis management system on both civilian and military sides. There are established documents to task and coordinate the stakeholders and ensure interoperability in national and international contingencies. SOPs and related equipment such as communication and transportation are employed in crisis management exercises either physically or in simulation centres. Joint planning is achieved through coordination and exercises of operation plans prepared by the civilian and military cells. Based on the outputs of those exercises, the interoperability and procurement requirements are developed. The Turkish procurement system refers to the interoperability criteria while supplying new capabilities.

The contribution from the military to a Comprehensive National Defence System through a UK lens is limited. A comprehensive national defence is more focused on a civilian lead with the military adopting a limited supporting role. The UK approach to national defence and how it is organised is predominantly expeditionary in nature which causes frictions in attempting to apply a Comprehensive National Defence System approach to existing force structures. Fusion Doctrine is the latest framework to cohere a cross-government response to securing national interests but remains an evolving model through which Defence must play an active part.

18.3 COVID-19 RESPONSE

18.3.1 Belgium

In the face of the COVID-19 pandemic Belgium established a Federal Coronavirus Task Force. Besides area-focused working groups, a group under the leadership of the Ministry of Defence was created to focus on logistics and distribution of medical and protective equipment and supplies. Equally important was the role of military commanders and their staff in provincial coordination mechanisms where they facilitated and coordinated requests for support, checking them against the support that the Ministry of Defence could effectively provide.

Most of the support provided was of medical nature and provided at the request of the FPS Public Health, facilitated by officers from Medical HQ embedded within the FPS Public Health as Liaison Officers. Together with the regional health inspectors, they determined the needs and priorities for defence support which were then sent to a specially created coordination cell at the Medical HQ that was responsible for the practical organisation of all the support provided by medical units.

The Ministry of Defence was tasked with the purchasing and the distribution of 18 million mouth masks and other medical equipment. For that purpose, a centrally located military base was assigned as the main logistical hub for the reception and the onward distribution towards eleven provincial military and civilian hubs. From these provincial hubs, equipment is further tested and distributed to users such as hospitals and retirement homes in collaboration with Civil Protection. The Ministry of Defence learned from the pandemic the benefit of at least one military base able to serve as a hub in each province.

Further, military ambulances and personnel were deployed to transport coronavirus patients to appropriate hospitals, medical personnel were also deployed in a supporting logistical role in retirement homes all over the country. The military hospital admitted all victims of acute burns – one of its core-competencies – from all around the country to free up resources in civilian hospitals. Wherever required, disinfection teams were deployed, as well as testing teams to directly test patients. Important activity was distributing equipment and supplies to the homeless in big cities and to centres for psychologically impaired and handicapped people.

In addition to medical support, the Military repatriated Belgian and European nationals' abroad, and supplies to the civilian airport of Liège which was a European hub for medical supplies.

Importantly, the military intelligence service and the civilian State Security Service had their role in combatting fake news and actors attempting to exploit the pandemic conditions.

Regarding the ongoing military operations, a variety of preventive and risk mitigation steps were taken such as pre- and post-deployment screening, pre-deployment isolation, reduced level of contact with people external to the mission, and within the Navy – cancellation of port calls and on-board quarantine.

18.3.2 Norway

The COVID-19 crises led to the shutdown of the Norwegian society from 12 March 2020 lasting several months. The authorities struggled to find a balance between preventing further increase of COVID-19 infections and at the same time sustaining vital societal functions. Many businesses and government institutions have increased working from home. This has led to widespread use of digital platforms for sharing information and conducting meetings, increasing digital vulnerabilities as well as straining the electronic communications infrastructure.

18.3.3 Turkey

The Turkish Armed Forces launched an initiative to overcome the challenges posed by the COVID-19 virus based on the motto "Training for Success, Measure for Health". The applied measures included cancellation of ceremonies, conferences, meetings, courses, fairs, and seminars, as well as postponement of national and international exercises. COVID-19 tests are periodically made in military units and centres. Medical staff in military units have been reinforced. For daily activities, it is mandatory to use masks and maintain social distancing. Disinfection measures are frequently applied while using weapons or other tools in military activities.

The Turkish Air Force has aided some NATO countries with medical supplies and essential equipment using A-400 transportation aircrafts.

18.4 FINDINGS AND RECOMMENDATIONS OF PHASE 2

18.4.1 Collaborative Defence: Exploring Relations and Expectations Between Society and Defence

As defence organisations are confronted with the need to constantly influence stakeholders on security policy, our study explores the main stakeholders for NATO and EU defence organisations as well as their connection to different comprehensive national defence frameworks. As we exploited the results of a systematic literature review, and base our findings on a unique set of 199 empirical papers, we add to parsimonious evidence-based insights characterising the field. After initially proposing a taxonomy dividing the most important stakeholders into stakeholder groups, we identified those stakeholder groups that were more (such as the Government including federal departments and ministries discussed in 68% of the papers)

or less prominent (such as first responders discussed in less than 2% of the papers). Thereafter we highlighted that, amongst the different frameworks being discussed, Total Defence (Zdanavičius and Statkus, 2020) [3] was the most studied framework whilst also exhibiting the highest number of linkages with the different stakeholder groups. This reflects its holistic nature and possible emergence as a baseline for future comprehensive national defence initiatives.

Further, whilst exploring some of the factors influencing the stakeholder network of defence organisations (such as the performance maturity level of the organisation, the country, and the armed force type), we were able to identify countries that are likely more advanced in the field with respect to others. We proposed that more ambitious armed forces that make greater use of performance measurement and management techniques may be better placed to leverage their stakeholder network. At the same time, our findings indicate that there may be room for defence organisations, especially those that are characterised by a lower performance maturity level, to expand their stakeholder network. However, there needs to be a balance between the ability of an organisation to process stakeholder complexity from within with respect to the "danger" of introducing even more complexity than can be handled. While additional research is needed on how organisations handle this trade-off (Hardy, Lawrence and Phillips, 2006) [2], too much focus on stakeholder engagement itself with respect to the stakeholder engagement capability of the organisation seems detrimental to organisation performance. There may therefore be a need for a progressive build-up of organisational stakeholder engagement capability preceding or accompanying consequential expansion in the stakeholder network linked to societal framework implementation efforts.

18.4.2 Cognitive Dimension of Comprehensive National Defence

The chapter about the cognitive dimension of comprehensive national defence describes the knowledge, views, and attitude required for this security concept at individual, organisational and societal levels. It builds on the premise that comprehensive national defence's ultimate aim is resilience to any crisis and an ability to resist the military and non-military aggression. The chapter outlines cognitive preconditions to develop and sustain resilience and resistance within the comprehensive national defence system. First, it is necessary to ensure that as many members of society as possible acquire basic military skills, emergency preparedness skills, civic skills, cyber security skills, media, information, and digital literacy. Second, within the scope of comprehensive national defence, long-term strategies must ensure trust in the armed forces, political trust, social cohesion, and realistic threat perception. Likewise, national strategic communication, education system, and overall state and society relations should strengthen national identity, national pride, and patriotism, which are essential emotional preconditions for society's willingness to defend a country.

18.4.3 Risk-Based Approach to National Security – Challenges and Recommendations

The Norwegian case study pointed to challenges related to protective security work and national security in light of increasing civil-military interconnectedness through globalisation and digitalisation of infrastructures and services [1]. The Norwegian Total Defence including the Armed Forces are subject to profound changes, both technologically, structurally, and organisationally. The new Norwegian security legislation was launched in 2019 to keep up with these developments. It includes modern risk management principles and shifts the balance form a predominantly rule-based to a risk-based approach. The Security Act puts forth that an *appropriate security level* shall be achieved, but does not answer what this level is, nor *how* to do this. Mission critically should guide prioritisation of security measures. Such a risk-based approach is nothing new. In the private sector, risk management and risk-based approaches to safety and security has been an integral part of enterprise management for decades. What is new is the shift toward such a regime in the defence sector.

The chapter establishes a hierarchy of national security values in accordance with the Security Act. Security measures must underpin mission objectives and operational capability, which again are crucial for national security interests. This hierarchy is a top-down translation of the desired political end state for national

security and defence tasks, down to military capabilities. A root cause for challenges related to protective security work and national security stems from complexity caused by increasing civil-military and public-private interconnectedness through globalisation and digitalisation of infrastructures and services. This leads to increasing structural, organisational, and technological complexity, and difficulty in obtaining necessary knowledge for risk assessment and management. Adaptation and development of new practices and necessary knowledge to implement a risk-based national security takes time. The only way to meet these challenges is by increasing knowledge and allocating sufficient resources to protective security work.

18.4.4 Better Aligned Comprehensive National Defence – A Challenge for Capability-Based Planning and Enterprise Architecture Methodologies

The research topic of the chapter emerged from the practical professional experience that cooperation between the state's different areas of responsibility in the context of comprehensive national defence could be improved.

As the defence domain has for some time already successfully implemented capability-based planning principles, which led to the question of whether the methodology of capability-based planning could work for other domains as well and how this could assist in improving the coordination of their cooperation. The study confirmed that the capability-based planning methodology could be applied together with the high-potential enterprise architecture methodology.

The chapter discussed the enterprise architecture, concentrating first and foremost on problems that could be solved with the methods based on enterprise architecture. The methodology, which was worked out in the 1970s and received its contemporary form in the 1980s, is successfully used in both private and public sector for over thirty years. Even though the content and application range of the methodology and the tools, based on the architectural framework, may vary, their internal logic still remains the same. They all allow handling complex organisations and their components as systematically organised elements so that important information and data are accessible to those concerned, is logically connected. This safeguards a constant overview of the organisation and its components and systematic administration of information and data, which enables it to carry out transitions, manage change and lead the organisation to achieve its goals.

The analysis demonstrated that in the case of implementing the methodologies in conjunction with each other the effect is greater than implementing each methodology on their own. The focus of each methodology is on establishing or maintaining the organisation, which corresponds to the vision and the set objectives. The emphasis of the methodologies, caused by their differences, showed that the methodologies rather contribute to each other than duplicate.

Capability-based planning methodology creates solutions for optimal use of existing resources and requires cooperation in cross-using capabilities. The solutions are made more comprehensively understandable for a broader range of users by including enterprise architecture methodology. Also, the capability-based solution architectures will have a more general usage in both the public and private sectors. Therefore, the hypothesis was confirmed that enterprise architecture is a suitable methodology for implementing capability-based planning methodologies.

The overall implementation of capability-based planning methodology allows estimating the number of capabilities in different domains whose fields of application go across sectors and which can be implemented to guarantee cost-effectiveness in performing various tasks. Hence it is possible to simultaneously ascertain and compare capabilities that are needed to perform the task with currently available capabilities and, if necessary, make amendments. Implementing a capability-based planning methodology across sectors gives us a general understanding of the situation regarding all existing and required capabilities. This creates a general knowledge of capabilities that can be shared with others or cross-used to avoid unreasonable duplication. By inserting the outcomes into the architecture framework, it becomes possible to create the

architecture of an organisation or domain that can help define the relations. In addition, architecture can assist in getting an overview of the current situation and drawing an implementation plan for future transitions and change.

18.4.5 Comprehensive Defence for City Security

City and urbanisation developed in parallel with human history. In the world of science, we see that the concept of city was firstly discussed in the East with Farâbî's "Al-Medinetü'l-Fâzıla" (The Virtuous City) and in the West with Plato's "Politeia". Max Weber, on the other hand, was the first sociologist to see the concept of the city as a living organism and connect modern society to urbanisation, defining property and personal rights, as well as city security and city law as essential elements for urbanisation.

In this study, when it comes to comprehensive defence for city security; the readiness of the city population to defend itself, facilitate crisis management, hybrid threats, local government's readiness during a crisis or other emergencies, energy supply, health, logistics, sustainability of city security capacity, economy and infrastructure, psychological resistance, etc. the adaptation of its functions to the process will be explained. These critical functions will be planned, coordinated, and implemented through local managing bodies, in partnership with private actors, Non-Governmental Organisations (NGOs), and residents. The goal of the comprehensive defence model for city security is to define specific defence responsibilities and the roles of managing bodies. Here, the goal will be to strengthen ties with the city population, business world, NGOs, and public administration and determine the stages. In the creation of a mutual trust, people must be brought together in different structures and thoughts close to each other. Comprehensive defence activities for city security; closer defence cooperation between the private and public sectors, courses that will increase patriotism awareness in schools, civil defence training and psychological defence training, as well as strategic communication, economic flexibility, security unit capacity building, cybersecurity will be carried out in the field. Assigning new duties and roles to public institutions according to their competence areas, determining the tools and roles that are vital in providing basic management functions during hybrid threats, potential crisis, or war, and raising awareness in urban residents will also be the most important stage of this process. By creating adequate frameworks and models, the state must resist attempts to spread disinformation by taking steps to ensure that the citizens of the city can self-organise and react when faced with difficulties.

18.4.6 Legal Aspects of Integrating Armed Forces into Internal Security Tasks

The Estonian case study takes the theory of "positivism" as its cornerstone for the analysis of the function of national legislation as the basis of ensuring the functioning of integration of cooperation between national defence forces and internal security forces. The function of law in such a system is to create norms that pertain substance of legal command and create procedural rules for the evaluation/application of said legal command. For the legal prescription pertaining to the either the rights and obligations of the defence forces of the state or powers enshrined in the internal security forces, every action ought to be evaluated based on the legality of the commands contained in the legal framework that creates the baseline for their actions.

Estonian legislation is analysed concerning how armed forces are integrated into the tasks of internal security forces. More detailing overview is given concerning the tasks of the Armed Forces, procedures, authorities and use of force.

18.4.7 Concept Model of Combined Headquarters

The concept of a combined headquarters springs from understanding that real-life comprehensive defence systems are complex endeavours consisting of a large number of diverse actors with often-conflicting objectives and perceptions operating under ambiguous command lines, which creates challenges in implementing the common tasks. Therefore, collaboration between stakeholders with underlying

C2 mechanisms, joint financing mechanisms, joint plans, and joint strategies is indispensable. Suggested uniform approach rests on five supporting concepts. The concept of escalation underpins the institutional dynamic of authorities and actions within the context of crisis management effort. A generic framework of levels of decision making enables the activities of military and non-military actors to be grouped and organised in a comprehensive manner. The concept of command and control agility addresses the flexibility and speed of coping with uncertainties and complexity of possible crises. The concept of crisis management phases deals with the volatility and unpredictability of the crisis and offers a holistic framework to address the continuum of events from pre-crisis to post-crisis status quo. Finally, the concept of stakeholders addresses the diversity and complexity of actors in the comprehensive defence system.

The main areas of responsibility of the network of Comprehensive Defence Headquarters (CDHQ) are crisis and emergency management, HNS, rear area security, and support of military operations as required. The role of CDHQ at the site level is to coordinate activities of contributing agencies as well as providing necessary horizontal and vertical liaison to other stakeholders. At the regional level, the role of CDHQ is overseeing ongoing resolve efforts of several simultaneous events and ensuring allocation and re-allocation of resources from contributing agencies available within the region to meet the evolving requirement in the field. At the state level, the CDHQ maintains situational awareness, oversees activities of regional-level CDHQs, allocates and re-allocates resources at state level to meet the evolving requirement and in accordance with policies, priorities and objectives established by the government-level political decision-making authority. National-level CDHQ could also have a responsibility to advise the political decision-making authority in their deliberations regarding policies, priorities, and objectives. The standardisation of procedures and reports, standardisation of communication and information exchange equipment, and standardisation of skills and knowledge through common training ensure the interoperability between different actors and decision levels. The required capabilities of the CDHQ are established using the NATO-agreed capability hierarchy.

18.4.8 Adaptation of Emerging Technologies into Defence

The 21st century can be considered as the revolutionary age of technology. We have seen some major advancements in the field of technology in the last decade and it is still going on at a rapid pace. The technology which is new today will become obsolete tomorrow given the speed of development with new concepts and techniques being invented every day. Emerging and disruptive technologies encompasses both new technology, and new use of existing technology, which will change the way we or potential adversaries operate. This includes ‘game-changing’ technology that revolutionises the field, but which could come with risks attached because it is new and untested. In this rising tide of revolutionary technology, the two most popular concepts which have gained the most attraction are AI (Artificial Intelligence) and Biotechnology including Human Enhancement.

Compared with conventional systems, military systems equipped with AI are capable of handling larger volumes of data more efficiently. Additionally, AI improves self-control, self-regulation, and self-actuation of combat systems due to its inherent computing and decision-making capabilities. Biotechnology will provide a new source to accelerate the development of weapons and equipment. For instance, the application of high-performance bionics and biomaterials could provide a new material basis for weapons and equipment, Human Enhancement Technologies (HETs) are biomedical interventions that are used to improve human form or to function beyond what is necessary to restore or sustain health. How successful the nation is in maintaining military superiority in an increasingly dangerous world will depend on how smartly the national leaders manage these tensions.

18.5 TOPICS FOR FUTURE RESEARCH

Throughout the country case studies, several themes and topics emerged that challenge the further development and implementation of the comprehensive defence concept. Although formulated in different ways in different case studies in this volume, the essence of identified themes could be distilled into the following shortlist:

- Search of the available literature with subject areas such as immunology and terms such as virus included into the results;
- Review and analysis of legal architecture in the field;
- Discussion of conceptually sound lead roles in different types of crises; i.e., which crises could be more effectively solved by civilian authorities with military support, and which crises could be more effectively solved by military authorities with civilian support;
- Discussion of the security architecture to support a coherent National Security Strategy;
- Discussion of the need for solid doctrinal base and standardised SOPs for the national crisis management system;
- Discussion of social cohesion and relations between society and state;
- Discussion of overcoming destructive trends in the information environment;
- Discussion of joint civil-military contingency planning, exercises, and competence enhancement;
- Discussion of resilience and redundancy.

The publication and dissemination of pre-released Phase 1 report ignited interest from outside the original research task group and the Chair received several requests to join the group to elaborate on a specific Phase 1-identified topic. As a result, the working group was expanded, and two extra chapters found their way to this volume. However, it is obvious that many of the problems identified in Phase 1 have not been thoroughly addressed in Phase 2 of the study. Also, insights into some of the identified challenges and problem areas have brought to light additional questions worth of research on their own right. Ongoing at the time of writing this report is Russian aggression against Ukraine. Many legal, institutional, and procedural solutions to outstanding and rapidly evolving National defence problems implemented by the Ukrainian government, as well as improvised on the ground by volunteers, provide rich empirical basis for further insights into, and analysis of, ways and means to implement the concept of comprehensive defence.

18.6 REFERENCES

[1] Endregard, M. (2020), “Norwegian case study”, Chapter 6, in NATO STO (2023), “Conceptual framework for comprehensive national defence system”, NATO STO Technical Report STO-TR-SAS-152-Part-I. Pre-release. NATO Science & Technology Organization, Neuilly-sur-Seine, France.

[2] Hardy, C., Lawrence, T. . and Phillips, N. (2006), “Swimming with sharks: Creating strategic change through multi-sector collaboration”, International Journal of Strategic Change Management, 1(1/2), pp. 96-112. doi: 10.1504/ijscm.2006.011105.

[3] Zdanavičius, L. and Statkus, N. (2020), “Strengthening resilience of Lithuania in an era of Great Power competition: The case for total defence“, Journal on Baltic Security, 6(2), pp. 1-21. doi: 10.2478/jobs-020-0009.

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's References	3. Further Reference	4. Security Classification of Document
	STO-TR-SAS-152 AC/323(SAS-152)TP/1010	ISBN 978-92-837-2330-1	PUBLIC RELEASE

5. Originator

Science and Technology Organization
North Atlantic Treaty Organization
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

6. Title

Conceptual Framework for Comprehensive National Defence System

7. Presented at/Sponsored by

Final report of Task Group SAS-152.

8. Author(s)/Editor(s)	9. Date
Multiple	May 2024
10. Author's/Editor's Address	**11. Pages**
Multiple	386

12. Distribution Statement

There are no restrictions on the distribution of this document. Information about the availability of this and other STO unclassified publications is given on the back cover.

13. Keywords/Descriptors

Civil resistance power; Comprehensive approach; Comprehensive defence; Crisis Management; Defence; Framework; Military; NATO; Security; Stakeholders; Systematic literature review

14. Abstract

To contribute to increased societal resilience and political-military situational awareness, the military must work with other actors within a framework that effectively combines political, civilian, and military crisis management instruments. As various models of comprehensive defence are implemented in different NATO member and Partner states, there is a need to study the conceptual underpinnings, as well as methods for planning, analysing, and validating the capability requirements and concepts of operation. This volume constitutes the final report of the SAS-152 study, comprising outlines of the study, followed by separate chapters reviewing available literature on the topic of comprehensive defence, and case studies arranged in alphabetical order of subject Nations. Based on preliminary findings from case studies, select aspects of the comprehensive defence concept are further addressed in multiple domains from multiple angles whilst using intellectual tools from multiple scientific disciplines. Finally, identified challenges and a list of topics to be further researched are provided in the last chapter.

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DIFFUSION DES PUBLICATIONS

STO NON CLASSIFIEES

Les publications de l'AGARD, de la RTO et de la STO peuvent parfois être obtenues auprès des centres nationaux de distribution indiqués ci-dessous. Si vous souhaitez recevoir toutes les publications de la STO, ou simplement celles qui concernent certains Panels, vous pouvez demander d'être inclus soit à titre personnel, soit au nom de votre organisation, sur la liste d'envoi.

Les publications de la STO, de la RTO et de l'AGARD sont également en vente auprès des agences de vente indiquées ci-dessous.

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivi du numéro de série. Des informations analogues, telles que le titre est la date de publication sont souhaitables.

Si vous souhaitez recevoir une notification électronique de la disponibilité des rapports de la STO au fur et à mesure de leur publication, vous pouvez consulter notre site Web (http://www.sto.nato.int/) et vous abonner à ce service.

CENTRES DE DIFFUSION NATIONAUX

ALLEMAGNE
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

BELGIQUE
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Bruxelles

BULGARIE
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2, 1592 Sofia

CANADA
DGSIST 2
Recherche et développement pour la défense Canada
60 Moodie Drive (7N-1-F20), Ottawa, Ontario K1A

DANEMARK
Danish Acquisition and Logistics Organization
Lautrupbjerg 1-5, 2750 Ballerup

ESPAGNE
Área de Cooperación Internacional en I+D
SDGPLATIN (DGAM), C/ Arturo Soria 289
28033 Madrid

ESTONIE
Estonian National Defence College
Centre for Applied Research
Riia str 12, Tartu 51013

ETATS-UNIS
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

FINLAND
Ministry for Foreign Affairs
Telecommunications Centre (24/7)
P.O Box 176, FI-00023 Government

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc
BP 72, 92322 Châtillon Cedex
O.N.E.R.A. (ISP)

GRECE (Correspondant)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HONGRIE
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25, H-1885 Budapest

ITALIE
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"

LUXEMBOURG
Voir Belgique

NORVEGE
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25, NO-2007 Kjeller

PAYS-BAS
Royal Netherlands Military Academy Library
P.O. Box 90.002, 4800 PA Breda

POLOGNE
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109,
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide, P-2720 Amadora

ROUMANIE
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street
Sector 6
061353 Bucharest

ROYAUME-UNI
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down
Salisbury SP4 0JQ

SLOVAQUIE
Akadémia ozbrojených síl gen.
M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIE
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55
1000 Ljubljana

SUEDE
Regeringskansliet,
Attn: Adam Hidestå
RK IF AR 5
S-103 33 Stockholm

TCHEQUIE
Vojenský technický ústav s.p.
CZ Distribution Information
Mladoboleslavská 944
PO Box 18, 197 06 Praha 9

TURQUIE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

AGENCES DE VENTE

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
ROYAUME-UNI

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2, CANADA

Les demandes de documents STO, RTO ou AGARD doivent comporter la dénomination « STO », « RTO » ou « AGARD » selon le cas, suivie du numéro de série (par exemple AGARD-AG-315). Des informations analogues, telles que le titre et la date de publication sont souhaitables. Des références bibliographiques complètes ainsi que des résumés des publications STO, RTO et AGARD figurent dans le « NTIS Publications Database » (http://www.ntis.gov).

NORTH ATLANTIC TREATY ORGANIZATION

BP 25
F-92201 NEUILLY-SUR-SEINE CEDEX • FRANCE
Télécopie 0(1)55.61.22.99 • E-mail mailbox@cso.nato.int

SCIENCE AND TECHNOLOGY ORGANIZATION

DISTRIBUTION OF UNCLASSIFIED STO PUBLICATIONS

AGARD, RTO & STO publications are sometimes available from the National Distribution Centres listed below. If you wish to receive all STO reports, or just those relating to one or more specific STO Panels, they may be willing to include you (or your Organisation) in their distribution.

STO, RTO and AGARD reports may also be purchased from the Sales Agencies listed below.

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number. Collateral information such as title and publication date is desirable.

If you wish to receive electronic notification of STO reports as they are published, please visit our website (http://www.sto.nato.int/) from where you can register for this service.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Royal High Institute for Defence – KHID/IRSD/RHID
Management of Scientific & Technological Research for Defence, National STO Coordinator
Royal Military Academy – Campus Renaissance
Renaissancelaan 30, 1000 Brussels

BULGARIA
Ministry of Defence
Defence Institute "Prof. Tsvetan Lazarov"
"Tsvetan Lazarov" bul no.2, 1592 Sofia

CANADA
DSTKIM 2
Defence Research and Development Canada
60 Moodie Drive (7N-1-F20)
Ottawa, Ontario K1A 0K2

CZECHIA
Vojenský technický ústav s.p.
CZ Distribution Information Centre
Mladoboleslavská 944
PO Box 18, 197 06 Praha 9

DENMARK
Danish Acquisition and Logistics Organization (DALO)
Lautrupbjerg 1-5, 2750 Ballerup

ESTONIA
Estonian National Defence College
Centre for Applied Research
Riia str 12, Tartu 51013

FINLAND
Ministry for Foreign Affairs
Telecommunications Centre (24/7)
P.O Box 176, FI-00023 Government

FRANCE
O.N.E.R.A. (ISP)
29, Avenue de la Division Leclerc – BP 72
92322 Châtillon Cedex

GERMANY
Streitkräfteamt / Abteilung III
Fachinformationszentrum der Bundeswehr (FIZBw)
Gorch-Fock-Straße 7, D-53229 Bonn

GREECE (Point of Contact)
Defence Industry & Research General Directorate, Research Directorate
Fakinos Base Camp, S.T.G. 1020
Holargos, Athens

HUNGARY
Hungarian Ministry of Defence
Development and Logistics Agency
P.O.B. 25, H-1885 Budapest

ITALY
Ten Col Renato NARO
Capo servizio Gestione della Conoscenza
F. Baracca Military Airport "Comparto A"
Via di Centocelle, 301, 00175, Rome

LUXEMBOURG
See Belgium

NETHERLANDS
Royal Netherlands Military Academy Library
P.O. Box 90.002, 4800 PA Breda

NORWAY
Norwegian Defence Research Establishment, Attn: Biblioteket
P.O. Box 25, NO-2007 Kjeller

POLAND
Centralna Biblioteka Wojskowa
ul. Ostrobramska 109
04-041 Warszawa

PORTUGAL
Estado Maior da Força Aérea
SDFA – Centro de Documentação
Alfragide, P-2720 Amadora

ROMANIA
Romanian National Distribution Centre
Armaments Department
9-11, Drumul Taberei Street, Sector 6
061353 Bucharest

SLOVAKIA
Akadémia ozbrojených síl gen. M.R. Štefánika, Distribučné a informačné stredisko STO
Demänová 393
031 01 Liptovský Mikuláš 1

SLOVENIA
Ministry of Defence
Central Registry for EU & NATO
Vojkova 55, 1000 Ljubljana

SPAIN
Área de Cooperación Internacional en SDGPLATIN (DGAM)
C/ Arturo Soria 289
28033 Madrid

SWEDEN
Regeringskansliet, Attn: Adam Hidestål
RK IF AR 5
S-103 33 Stockholm

TÜRKIYE
Milli Savunma Bakanlığı (MSB)
ARGE ve Teknoloji Dairesi Başkanlığı
06650 Bakanliklar – Ankara

UNITED KINGDOM
Dstl Records Centre
Rm G02, ISAT F, Building 5
Dstl Porton Down,
Salisbury SP4 0JQ

UNITED STATES
Defense Technical Information Center
8725 John J. Kingman Road
Fort Belvoir,
VA 22060-6218

SALES AGENCIES

The British Library Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
UNITED KINGDOM

Canada Institute for Scientific and Technical Information (CISTI)
National Research Council Acquisitions
Montreal Road, Building M-55
Ottawa, Ontario K1A 0S2, CANADA

Requests for STO, RTO or AGARD documents should include the word 'STO', 'RTO' or 'AGARD', as appropriate, followed by the serial number (for example, AGARD-AG-315). Collateral information such as title and publication date is desirable. Full bibliographical references and abstracts of STO, RTO and AGARD publications are given in "NTIS Publications Database" (http://www.ntis.gov).

ISBN 978-92-837-2330-1