



Commanders' and Staff

Capstone Handbook for Attacking the Networks (AtN)



3400 TSX FCX 0010/TT-10533/Ser:NU0454

TO: See Distribution

SUBJECT: Commanders' and Staff Capstone Handbook for Attacking the Networks (AtN)

DATE: 28 May 2014

1. The Improvised Explosive Device (IED) has become the preferred weapon of insurgents, terrorists, and other irregular threats in conflict and remains a serious challenge in the future. These irregular threats employing IEDs are predominately associated in transnational and regional networks. In order to effectively meet and mitigate this challenge, NATO must remain adaptable and flexible while developing effective and robust Counter-IED (C-IED) policies and procedures for current and future operations. C-IED activities must also be widely understood, integrated and institutionalized across all levels of command, especially Intelligence and Operations, and not relegated to a specialist functional area.

2. As directed by the North Atlantic Council in the NATO C-IED Action Plan Revision 1, dated 25 Oct 13, and the Bi-Strategic C-IED Campaign Plan, dated 27 July 13, Attacking the Networks (AtN) that can facilitate IED use is the NATO C-IED main effort. AtN is the proactive approach of physical and cognitive activities required to interdict threat networks, reinforce friendly networks, and influence neutral networks. This approach is necessary if NATO is to maintain operational and strategic freedom of action and support the Alliance's center of gravity. The *Commanders' and Staff Capstone Handbook for Attacking the Networks (AtN)* is provided at Enclosure 1 and has been developed to provide guidance on "what needs to be done, and why" rather than "how to do it." This handbook was developed from hard learned lessons from over a decade of conflict and with input from ISAF and National publications and experience.

3. NATO organizations and Nations are encouraged to disseminate the handbook widely. They are also invited to submit feedback, in support of periodic revisions of the document, to the ACT C-IED Integrated Product Team Leader, LtCol Kevin Scott, Kevin.Scott@act.nato.int; +1-757-747-4244.

FOR THE SUPREME ALLIED COMMANDER TRANSFORMATION



Phil Jones CBE
Lieutenant General, GBR A
Chief of Staff
Allied Command Transformation

ENCLOSURE:

1. Commanders' and Staff Capstone Handbook for Attacking the Networks (AtN).

DISTRIBUTION:

External –

Action:

SHAPE (Attn: COS, NMRs)
JFCBS
JFCNP
LANDCOM
MARCOM
AIRCOM
NSHQ
COS ISAF
COS IJC
C-IED COE
HUMINT COE
DAT COE
CSW COE
NMIOTC
JAPCC
JCBRN COE
NATO JEWCS
USJS J7
Non-NATO ISAF Troop Contributing Nations MODs

Internal –

Action:

MPD

ACT Distribution list II

ACT Distribution List III – National Liaison Representatives

ACT Distribution List V – PFP Staff Element (PSEs)

ACT Distribution List VI – PFP National Liaison Representatives

Information:

DCOS CD

DCOS JFT

DCOS SPP

**Intentionally
Blank**

Preface

Aim

1. The aim of this handbook is to provide Commanders and Staff with a concise, easily referenced document to assist them in understanding, planning and conducting operations against threat networks that can facilitate the use of IEDs.

Purpose

2. The purpose of the handbook is to assist in establishing and solidifying, within all levels of the NATO Alliance, the general concepts of attacking and countering threat networks. This will enhance NATO capability in its core purpose of guaranteeing the freedom and security of its members through political and military means.

Scope

3. The handbook describes the analytical methodologies that form the basis for identifying threat network vulnerabilities that can then be exploited. It recommends options, functions, and activities to engage the threat networks in order to proactively degrade the adversary's freedom of action. An understanding of the adversary's motivation, organizational design and activities will enable effective operations to isolate and neutralize those identified organizational functions.
4. This handbook will further explain Attack the Network (AtN) activities as defined in AJP-3-15(B) within the broader context of Countering Threat Networks (CTN) as outlined in the NATO Joint Analysis and Lessons Learned Report on AtN dated 3 Aug 2013.
5. Although this handbook will describe countering threat networks from a C-IED perspective, there is a broader application that applies to any adaptive, irregular threat network (e.g. terrorism, proliferation, cyber, smuggling, human and narco-trafficking etc.) that may challenge Alliance forces engaged across the range of military operations, from Cooperative Security, Crisis Management, through to Major Combat Operations needed for Collective Defence.
6. The handbook covers the whole range of military operations and spectrum of conflict.

Background

7. Adaptive, irregular threat networks will remain a potential threat across the full range of Alliance operations. Activities in support of attacking and countering threat networks never stand alone. Commanders must integrate these activities into intelligence preparation of the operational environment and into pro-active, all-encompassing actions. This will reinforce and support the overarching operations or campaign plan. The overall objective of AtN activities is to reduce the capability, functionality and activity of threat networks to a level that is manageable by the Alliance or the host nation/civil authority that the Alliance is supporting. Fundamentally, this is accomplished by:

- a. Supporting and developing the capabilities of friendly networks.
- b. Positively influencing neutral networks.
- c. Interdicting, neutralizing, isolating, and exploiting threat networks of all types.
- d. Continuously protecting the force and population while carrying out the above functions.

8. The NATO AtN definition in countering IED is to:

“Isolate the component parts of the networks through the coordinated and selective use of cognitive and physical activities to defeat the Improvised Explosive Device (IED) System.”

9. Inherent within the AtN definition is the offensive nature of these physical and cognitive activities in order to shape the networks permeating the Joint Operational Area (JOA) and broader Operational Environment (OE). This allows operational or campaign objectives and end-states to be achieved, as well as managing the threat networks to a point where defensive and force protection measures can provide maximum effectiveness. The offensive connotation of the term “Attack” has to be understood in its wider capabilities to be applied.

10. Critical to supporting effective AtN is the strategic ability to counter threat networks. The term, “Countering Threat Networks” (CTN) has a broader meaning that describes all the activities, principally civilian, that attempt to prevent, deter, pre-empt, interdict and respond to networks that can facilitate the use of IED. CTN is not yet an approved NATO concept, but because regional and transnational threat networks do not constrain themselves to geographic boundaries, NATO must address the totality of the

threat networks' span of activities and influence in order to deny threat networks sanctuary and to be effective within the JOA.

11. The aims, as well as the strategic approach of CTN, are inextricably linked and complimentary to AtN and are to:

- a. Interdict, neutralize, isolate, and exploit threat networks within the NATO Area of Interest (AI) while supporting Attacking the Networks (AtN) to accomplish the same within established JOAs.
- b. Support and reinforce Alliance friendly (Allied, Partner, non-military) networks against threat networks – effectively, this is the Alliance transformational main effort.
- c. Influence (through public affairs and diplomacy, CIMIC, counter threat finance, cyber, etc.) neutral networks in order to increase their support to NATO objectives while in parallel, reducing their support/indifference to threat networks.

13. Consequently, the purpose of AtN as well as CTN is to:

- a. Prevent, deter, pre-empt, interdict, and respond to threat networks.
- b. Improve NATO force freedom of action.
- c. Protect the Alliance Centre of Gravity defined as Alliance cohesion.
- d. Contribute to collective and homeland security.

14. The CTN working description is:

The non-military lead actions to counter threat network activities in the Area of Interest (AI) and the strategic support to military Attacking the Networks (AtN) efforts in the Joint Operational Area (JOA) through the employment of the Comprehensive Approach.” (Detailed in Paragraph 16)

15. CTN is a Critical Requirement to ensure success of military led AtN within the JOA. Conversely, AtN is also an enabler for effective civilian (Law Enforcement, Diplomatic, Financial, etc.) led CTN activities in the AI. AtN and CTN commonalities abound. Both efforts are intelligence/evidence based and they both rely on forensic and biometric information gleaned through exploitation and recovery. Both require significant information exchange and sharing between military and civilian organizations across tactical, operational and strategic levels.

16. In military terms, AtN can be seen as “close operations” in the conflict area and CTN as “deep operations” in the AI. Conversely, from a national perspective, activities against threat networks are a civilian, law enforcement led, close operation that will be significantly enhanced by CTN in the Alliance AI.

17. AtN is a subset of CTN that, when appropriately synchronized with CTN, produces a single battle/conflict space concept that encompasses the entire operational area of the threat networks. The important difference between the two lies in how the JOA and AI are defined, the established command and control relationships (AtN – military led, CTN – civilian led), and the interdiction methods (AtN – kinetic and non-kinetic, CTN – overwhelmingly non-kinetic law enforcement activities). The two concepts are interdependent and complimentary (See Figure 1).

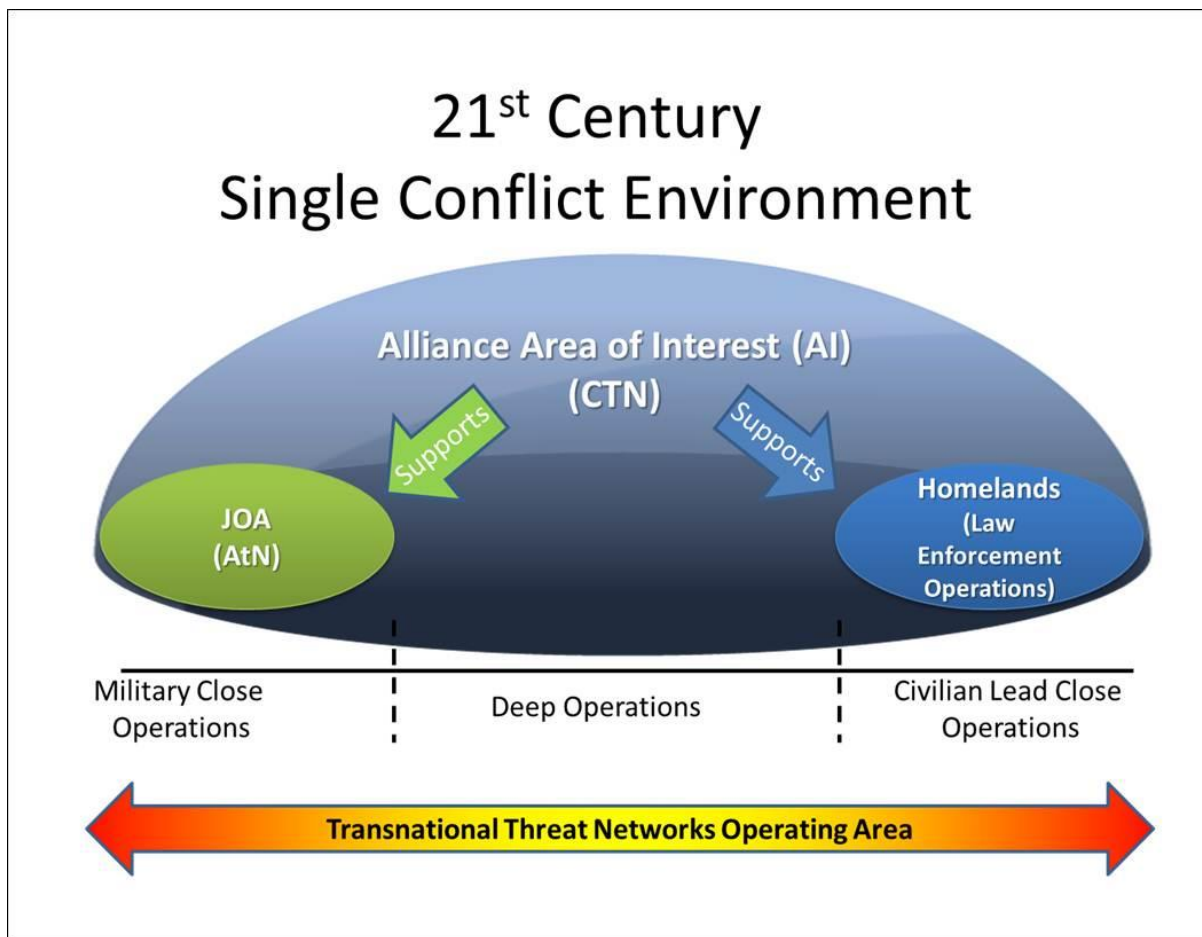


Figure 1 - AtN vs. CTN within the AI

Comprehensive Approach

18. The Alliance must employ a comprehensive approach to conduct AtN (as well as CTN) activities and operations. These activities and operations cover both lethal and non-lethal actions, directed against networks of human actors. The aim is to reduce the networks' ability to negatively affect the operational goals of Alliance forces, and to ultimately neutralize those networks. This approach includes a requirement for coordinated action from an appropriate range of civil and military actors, enabled by the orchestration, coordination and de-confliction of NATO's political and military instruments with other instruments of power.

19. NATO's engagement in a comprehensive approach to crisis management is focused at three levels:

- a. At the political and strategic level, NATO concentrates on building confidence and mutual understanding between international actors.
- b. At the theatre level, NATO force commanders must be empowered to conduct effective cooperation and coordination with indigenous local authorities and other international actors in the execution of operations.
- c. At the operational level, the priority is to cooperate with other international actors in the overall planning for complex operations in which a large degree of civil-military interaction will be required.

Note: All 3 levels must function in a complimentary manner to achieve success.

20. The comprehensive approach for AtN/CTN operations would include the end-to-end integration of command and control, intelligence, movement and manoeuvre, fires, protection, sustainment, and special operations capabilities with non-military elements of power including public diplomacy, economic, financial, and legal/law enforcement means. In this era of failed states, destabilizing elements, and high-end irregular, asymmetric threats, this would enable the Alliance to establish and maintain continuous harmonized pressure against any combination of threats to the Alliance including, but not limited to, insurgents, terrorists, crime groups and state sponsored or transnational actors across the continuum of operations in all levels of conflict.

21. The Alliance must be prepared to adapt rapidly to each specific threat in all phases across the spectrum of conflict. Successful operations will require the Alliance to work closely with, provide support to, and receive support from, our non-military, international partners. This is not a fight NATO can win on its own but only through the application of all aspects of combined international power across the OE -- both within the JOA as

well as in the Area of Interest. Identifying and defining specific threats will become increasingly difficult but is absolutely necessary if the Alliance and its partner nations' aim to counter the threats those organizations pose to local and regional and global stability.

22. NATO's operational planning, intelligence and targeting processes¹ are already in place and generally cover most of the steps needed within the JOA for the AtN process. However, not only are these processes not yet harmonized, but a broader comprehensive approach to address the threat networks outside of the JOA that influence threat activities within the JOA is lacking.

Summary

23. The majority of the current threats facing the Alliance and its regional partners are in fact organized networks with established and identifiable infrastructures.

24. These networks are adapted to their operational environment and are capable of surviving and accommodating substantial military and political changes in that environment. The vast majority of these networks are adaptive and designed to survive.

25. Neutralizing threat networks is not an easy task and requires an intense intelligence collection/analysis and fusion effort. This has to be allied with patience, and an integrated, synchronized, cooperative offensive effort on the part of the Alliance, numerous civilian governmental and non-governmental entities.

26. By identifying a threat network's motivation, constituent components and critical functions, we can develop a range of physical and cognitive (lethal and non-lethal) options that can be applied in all operational phases and at multiple levels (tactical, operational, and strategic), that capitalize on, or create adversaries' vulnerabilities, that the Alliance then can leverage to interdict and neutralize these threat networks to foster Alliance objectives and protect Alliance cohesion.

¹ ACO Comprehensive Operational Planning directive COPD 17 Dec 2010, AJP3 AJP 2.1(A) Intelligence Procedures dated September 2005, ACO Directive (AD) 80-70 - Campaign Synchronization and Joint Targeting in ACO, dated 27 April 2010 and AJP-3.9 Allied Joint Doctrine for Joint Targeting, dated 22 May 2008.

Table of Contents

PREFACE.....	4
Aim.....	4
Purpose.....	4
Scope.....	4
Background	5
Comprehensive Approach	7
Summary	9
TABLE OF CONTENTS.....	12
CHAPTER 1 – THE DYNAMIC OPERATING ENVIRONMENT	14
Introduction	14
Networked Threats to Stability	15
Adaptive Networked Threats.....	16
CHAPTER 2 – OVERVIEW OF THE ATN/CTN METHODOLOGY IN THE OPERATIONAL PLANNING PROCESS (OPP)	21
NATO AtN/CTN in Joint Operations	21
NATO AtN/CTN Fundamental Actions.....	21
Influence Neutral Networks and Exploit All Opportunities with Information Operations (IO)	28
Interdict, Neutralize, Isolate and Exploit Threat Networks	30
CHAPTER 3 – UNDERSTANDING ADAPTIVE THREAT NETWORKS	32
Introduction	32
Threat Network Characteristics	33
Network Strengths and Weaknesses	35
Identifying and Defining a Network	36
Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR)	45
CHAPTER 4– ENGAGING ADAPTIVE THREAT NETWORKS	48
AtN/CTN Engagement Overview.....	48
Engaging Networked Threats at Each Level of Conflict	49
Targeting the Network	53
Target Types	53
Targeting Methodologies	55

Fixing and Finishing Options.....	58
Assessment	60

CONCLUSION	61
------------------	----

CHAPTER I

THE DYNAMIC OPERATING ENVIRONMENT (OE)

Introduction

1. NATO faces a broader and less well defined range of complex security threats today than it did when the Alliance was formed. These threats are further complicated by the requirement for NATO to protect and defend against threats from both state and non-state actors as well as being threatened from within the JOA and now having homelands and rear staging areas threatened by asymmetric capabilities beyond the JOA. Alliance forces will operate in an international environment where struggle predominates. The dynamic nature of this OE has significantly altered the face of conflict and the Alliance's decision cycle. While the origins of war may rest on policy, a variety of factors has influenced the conduct of that struggle in the past and will do so in the future. The tension between rational political calculations of power, on one hand, and secular or religious ideologies on the other, combined with the impact of passion and chance, makes the trajectory of any conflict difficult if not impossible to predict in today's OE.

2. Consequently, whereas the 20th Century operating environment was generally linear and physical in nature, with recognized bi-polar competition between recognized nation states, the dynamic operating environment of the 21st century is defined as multidimensional, technological and information super-empowered, fast-paced, and culturally based upon human dynamics.

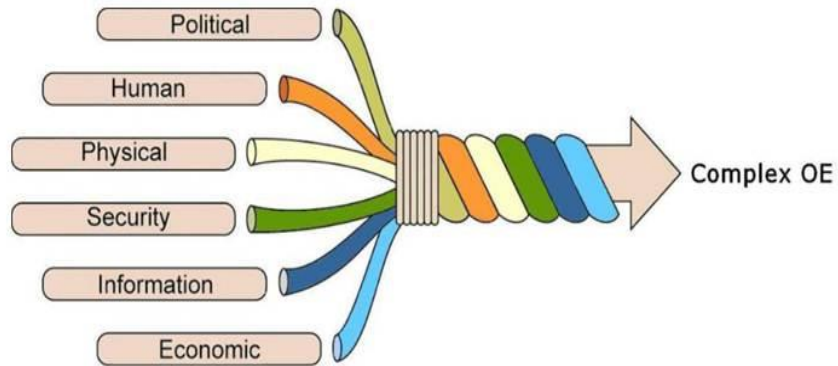


Figure 2 - Variables of the Operating Environment of the 21st Century

Networked Threats to Stability

3. In the future, non-conventional or irregular, non-state, regional, or transnational threat networks will represent a significant threat to NATO. They include insurgents, terrorists, criminals, weapons traffickers, etc. These networks embrace asymmetric means to harm nations and the Alliance and have recognized the benefits of using the IED as a tactical, operational and strategic weapon of influence.

4. The IED has become a weapon of choice for many reasons but mainly due to ease of manufacturing, simplicity of employment, low cost, lethality, anonymity, dramatic propaganda effects, and the challenges the Alliance faces in countering the weapon and tactic without extraordinary means. Its effectiveness as a weapon system provides threat networks with a capability whose effect is massively, and favourably, disproportional to the effort needed to employ it against the Alliance and our Partners. However, since the threat networks that facilitate the employment of IEDs operate not only within the military AO, but significantly within the Alliance (global) AI, they represent not just a military challenge, but also contains political, legal, Informational, financial, and diplomatic aspects that NATO's C-IED efforts must also take into account.

5. It is widely accepted that future adversaries, specifically networked adversaries, will often operate across borders, and even globally. These groups may conduct long-term operations and campaigns with aims we traditionally do not understand or track. Their approach poses challenges to the arrangement of nation states and national

capabilities aimed at mitigating their actions, whether it is law enforcement organizations, military organizations, or other state actors.

6. These trends, whether they adhere to predictions or not, will combine in ways that form broader and more robust networked contexts that will define the world in which the NATO Joint Force will operate in the future. Consequently, whether they combine to form a hybrid threat, (defined by the US Army as *“the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects”*)² or as individual malign networks, NATO commanders and forces will be compelled to address threats as networks, rather than as the easily recognizable linear forces of the 20th Century. Understanding networks and how to attack the malign ones will be critical to the future success of NATO.

Adaptive Threat Networks

7. A network is a series of direct and indirect ties [links] from one actor [node] to a collection of others. Networking extends the range and variety of both their military and political actions.³

8. A human network is an alliance of socially connected individuals who are involved in activities to achieve some form of social, political, monetary, religious, or personal gain. Networks are comprised of nodes, links, and cells that support a variety of functions and purposes. The network can also have members that are unaware of illicit activities and the true aim of the network. As such, a node may fall into one or more network types at any given time, making definition and categorization of a network difficult. Typical descriptions of network structure are noted in Figure 3 and Figure 4 illustrates some of the basic structure.

² US Department of the Army. (2010). *TC 7-100 Hybrid Threats*

³ U.S. Joint Operation Planning JP 5-0

Nature of Network Bonds

The following descriptions of network structure are derived from the London (United Kingdom) Metropolitan Police Service's definitions of networks. The Criminal Intelligence Service Canada, Central Bureau, added the "specialized network" to capture another dimension of criminal interactions. All of these structures "can be organized in a non-hierarchical, non-contiguous network of cells."

Family: Some members or associates have familial bonds. These bonds may be cross-generational.

Cultural: The network shares bonds due to a shared culture, language, religion, ideology, country of origin and/or sense of identity. Some of these networks may evolve over time from being culturally to proximity based.

Proximity: The network shares bonds due to certain geographical ties of its members (ex. past bonding in correctional or other institutions, or living within specific regions or neighbourhoods). Members may also form a network with proximity to an area strategic to their interests (ex. a neighbourhood or key border entry point). There may be a dominant ethnicity within the group, but they are primarily together for other reasons.

Virtual: A criminal network that may never physically meet but work together through the Internet or other means of communication (ex. networks involved in online fraud, theft, or money laundering).

Specialized: Individuals in this network come together to undertake activities primarily based on the skills, expertise or particular capabilities they offer.

Figure 3 - Illustration of basics of networks' structure

9. In order to more easily categorize networks for the sake of AtN/CTN, networks are segregated into one of three broad areas:

- a. Friendly networks - (NATO, Troop Contributing, and legitimate Host Nation Forces)
- b. Neutral networks - (Indigenous populations, Non-governmental Organizations, international audience)
- c. Threat networks - (Proxy Nation, Insurgent, Terrorist, Criminal)

10. A friendly network is a network with goals or objectives that are aligned with Alliance interests and generally support the Commander's operational goals. Examples include host nation police forces, armed forces, government officials, supportive business and social leaders, and active or passive supporters or sympathizers among the host nation population. Friendly networks are often referred to as 'blue' (NATO forces) and 'green' (Host Nation forces) in current operational contexts based upon NATO standard map symbols' colouring. NATO COIN doctrine AJP3.4.4 places these actors in the "positive" category based on their aims, methods and relationships.

11. A neutral network is a party identified as neither supporting nor opposing friendly or enemy forces. In the context of AtN/CTN, a Neutral Network (white) neither actively supports nor opposes Alliance interests and does not negatively impact the Commander's operational goals. A neutral network is generally not considered a current threat or asset to the Commander and should be a significant focus of resources in order to influence the network to support the Commander's goals, effectively converting them to a friendly network. NATO COIN doctrine places these actors in the "neutral" category based on their aims, methods and relationships.

12. A threat network can be an enemy (overtly hostile), adversary, criminal, or any combination thereof. A Threat Network is a network with goals or objectives that actively oppose Alliance interests, negatively influence or impact the Alliance's strategic, operational, or tactical goals, and have a malign effect on the dynamic operational environment. Threat networks are most commonly referred to as 'red' if they clearly represent networks actively in hostile opposition to NATO objectives or "black" if they indirectly have negative effects, such as criminal organizations, on NATO goals and objectives. NATO COIN doctrine divides these actors in two categories either "negative" or "hostile" based on their aims, methods and relationships. Negative actors oppose Alliance or Host Nation authority but stop short of violence. Hostile actors actively and violently oppose Host Nation or NATO forces.

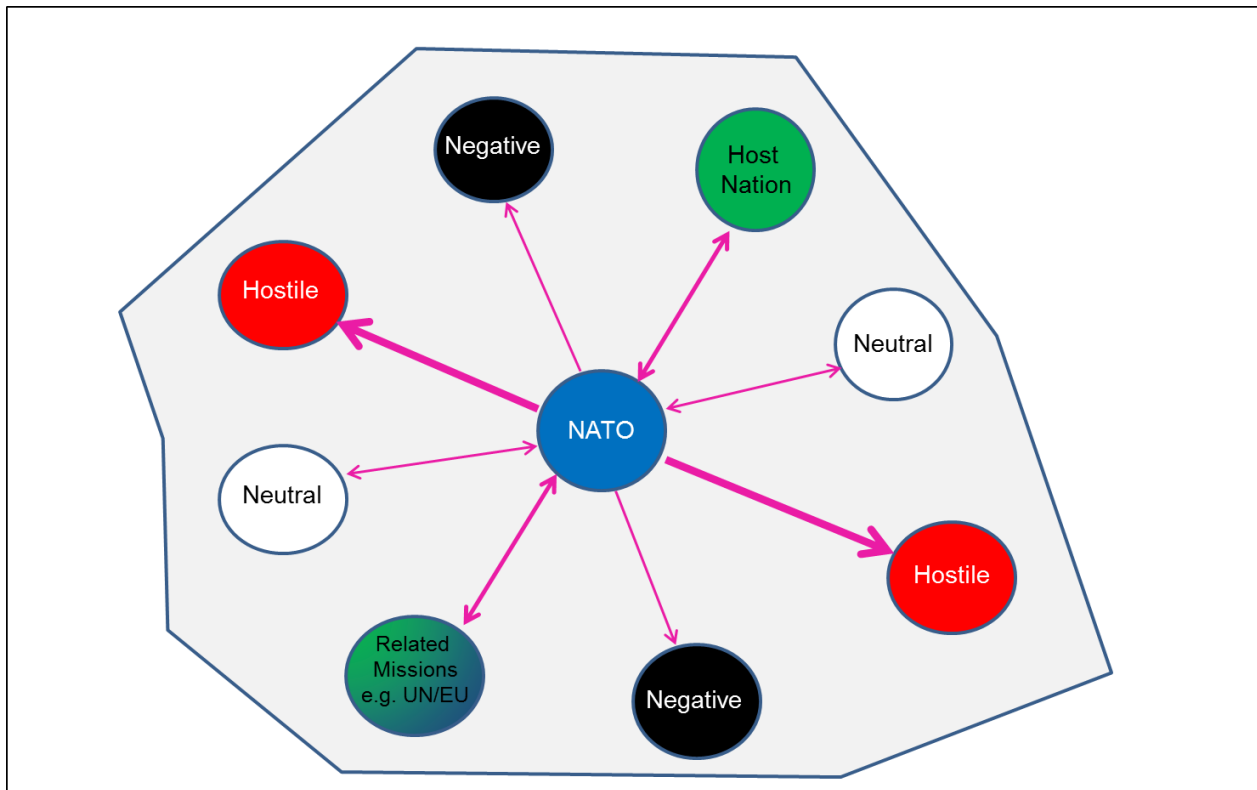


Figure 4 - NATO may have to deal with several different types of networks within the JOA

13. Threat networks exhibit unique characteristics that must be considered when deciding how to effectively engage them. These characteristics make them very resilient and require understanding if the commanders' actions are to achieve their desired effects. These characteristics are more evident in the JOA during AtN operations than in CTN operations outside the JOA:

- a. **Co-Adaption** – An organization that adapts to something that is adapting to it.
- b. **Emergence** – emergence allows collections of apparent unimportant, dumb or ignorant single components to behave in very intelligent ways as a system.
- c. **Self-Organizing** – Ability of a system to organize without a central authority or external element imposing structure upon it through planning.
- d. **Regenerative** – components are easily replaced within the system

e. ***Decentralized (Flat)*** – System in which the capabilities are distributed throughout the system or network. In such organizations, relationships are key and the network relies on its relationships (links) to function

14. Generally speaking, these networked threats share the same characteristics as those described in NATO COIN doctrine⁴ for insurgent networks:

- a. A decentralized non-hierarchic structure.
- b. Shared identity among the membership normally based on kinship/tribe, ideology, religion and personal relations, which also facilitates recruitment.
- c. Knowledge, skills, and abilities of group leaders and members.
- d. Resources in the form of arms, money, social connectivity and public recognition.
- e. Adaptability including the ability to learn and adjust behaviours and modify Tactics, Techniques and Procedures (TTP) in response to friendly initiatives, reactions and countermeasures
- f. Have access to a sanctuary to conduct planning, training and logistic reconstitution.

15. Understanding the types and functions of the networks that comprise the dynamic OE in the Alliance AO as well as the AI, is a critical first step in the AtN process.

16. Successfully exploiting an adversary's network is very difficult; however, there are certain critical functions that are common to all networks that may be identified and exploited or attacked. These functions are performed by key individuals who are also subject to discovery and exploitation. Thus targeting individual functions such as those associated with an IED support network also affect the rest of the adversary's operational infrastructure. Actions to attack critical network functions must be synchronized and integrated with the overall operations campaign against the adversary. Joint force targeting efforts must employ a multi-echelon, holistic approach; leveraging lethal and non-lethal capabilities that keep continuous pressure on multiple functions within the network's infrastructure.

⁴ AJP 3.4.4 COIN Doctrine

CHAPTER II

OVERVIEW OF AtN/CTN METHODOLOGY in the OPERATIONAL PLANNING PROCESS (OPP)

NATO AtN/CTN in Joint Operations

1. Attack the network (AtN) activities are nested within the broader joint operation/campaign planning, execution, and assessment processes (e.g., JIPOE, operational art/design, OPP, targeting). In short, AtN (and CTN) is the integration of actions conducted across all elements and levels of the Alliance, including Joint Force/non-military elements of the international community and host nation partners, as applicable, to neutralize threat networks and to enhance friendly and neutral networks. AtN(and CTN) activities include:

- a. Fusing intelligence.
- b. Operational manoeuvre.
- c. Engaging targets with lethal and non-lethal fires to influence:
 - (1) Leadership, financial support, strategic communications, recruitment, command and control, and other significant nodes.
 - (2) Local support/infrastructure base.
 - (3) Logistic channels.
 - (4) Materiel and manpower resources.

2. The AtN(and CTN) methodology, discussed in Paragraph 3 below, is designed to enable a commanders and staffs from the tactical through strategic to fine tune its understanding of how threat networks operates and to neutralize its ability to efficiently and effectively conduct its activities. It should be noted that merely neutralizing or destroying a portion of a threat network does not guarantee lasting success. Many networks reconstitute or move to a new location. Lethal and non-lethal engagements against the conditions within the OE that allow the threat networks to operate set the conditions that render the threat irrelevant and achieve the commander's intent. In COIN operations, for example, successful lethal and non-lethal engagements, to clear

the enemy from an area, allow friendly forces to hold and build. This provides the host nation (HN) government with the opportunity to restore rule of law, provide necessary infrastructure, and reduce support for the enemy's activities; thereby fundamentally altering the OE in favour of friendly forces. Ultimately, AtN and CTN activities are designed to neutralize the threat networks, create the conditions that enable friendly networks to effectively function with the support of the local population, and establish the conditions that will allow the disengagement of Alliance forces.

NATO AtN and CTN Fundamental Actions

3. AtN and CTN involves more than the focused use of ISTAR assets, analytical methodologies, and dynamic or deliberate targeting means. If AtN/CTN is to make a contribution to the success of the overall joint operation/campaign, it must be a part of a broader, command wide effort to:

- a. Support and reinforce friendly networks,
- b. Influence neutral networks,
- c. Interdict/neutralize/isolate and exploit threat networks.

These fundamental actions leverage the lethal and non-lethal capabilities of the military force, participating non-military, and HN partners.

4. Fundamental actions will include:

a. *Support and Reinforce Friendly Networks.* Unified action is employed to shape and strengthen the friendly network to the benefit of friendly forces and the detriment of the threat network. The Alliance commanders and staffs must first design a joint operation/campaign that reflects their understanding of the OE in order to "build a better network." This sets the conditions for a fully partnered AtN/CTN planning and execution that can effectively support rapid decision-making and synchronize military and civil actions. This also enables units and commanders to take advantage of fleeting opportunities and to quickly identify and take educated tactical risks. Specific actions to accomplish this task include:

- (1) Ensure caveats and Memorandums of Agreement (MOA) clearly articulate the capabilities resident on the Alliance Force task organization.
- (2) Understand the contributions of each element involved in the AtN/CTN effort.

- (3) Ensure that there are simple command and control arrangements in place to maximize unity of effort.
- (4) Clearly understand what capabilities are not available in each organization on the task organization.
- (5) *Ensure that information-sharing mechanisms are in place and that they are flexible and understood by all entities and organizations involved in the AtN/CTN effort(s).*
- (6) Maximize Liaison Officer exchanges.
- (7) Incorporate, from the beginning, vetted Host Nation/Partner Nation forces into the task organization.
- (8) Incorporate, as early as possible, civil and international non-military considerations into planning and ensure a comprehensive approach to operational design.

b. *Provide Commander's Guidance.* The Joint Force will initially conduct a brief evaluation of the mission and provide initial planning guidance to the staff. At a minimum, very early in the mission analysis process, the intelligence staff must ensure that the Joint Force is aware of the capabilities and intent of the various actors that comprise the threat networks, current status of friendly networks, and current posture of the neutral networks. This will assist the JTF in formulating initial commander's guidance, which normally initiates the mission analysis and planning process. Key elements that result from mission analysis and the planning process include a draft mission statement, commander's intent, and concept of operations (CONOPS). There will be no CDR's guidance for civilian led CTN efforts outside the AI, so in these cases military organizations should seek out common objectives among the various stakeholders and strive for unified action against transnational threat networks.

c. *Conduct Operational Design.* Operational design enables the Joint Force and staff to outline a strategy for reaching a sustainable end state in the operational area. An outcome is the development of Lines of Effort (LOE) that are further developed into intermediate objectives and desired effects with supporting measures of effectiveness (MOE) and measures of performance (MOP). This ensures commanders and staffs at each echelon are planning and executing operations across all LOEs that support achieving the same overall end state. Continuous assessment is required to identify and adapt to changing conditions. Additionally, linkages between unit plans' defining intermediate objectives for all

LOE and the commander's critical information requirements should be established to focus units on collecting information that commanders at all levels will use to make timely and accurate decisions. Incorporating AtN/CTN based decisive points into the LOE is critical to influencing the operational design of campaigns in the current dynamic OE.

d. *Establish and Standardize Targeting Processes.* The Joint Force identifies the focus for the targeting cycle and promulgates this in the commander's initial guidance and commander's intent. The targeting process is designed to transform intent into reality through the identification of the human, material, or other capital which the adversary networks need for the successful execution of their operations. The targeting process is designed to ultimately identify the high-payoff targets (HPTs) that must be addressed to achieve friendly success and the high-value targets (HVTs) the loss of which would seriously degrade the threat networks. Moreover, a significant modification of this process for AtN/CTN not only incorporates the numerous forms of network analysis (discussed in Chapter III), but the targeting process must include non-kinetic targeting to address the AtN/CTN plan objectives of influencing neutral networks (as well as threat networks). The targeting process is focussed on achieving effects and employing the best instruments to achieve those effects. The NATO Commander's and Staff Handbook for C-IED provides recommendations on how to organize for these activities.

e. *Empower Information Exchange.* Vertical and horizontal knowledge sharing is essential in planning and execution. Sharing operational knowledge and intelligence simultaneously across the entire friendly network, through a comprehensive approach⁵ to create a common understanding of the OE, and specifically the threat networks, enables the friendly network to out manoeuvre the threat networks through information dominance. This shared understanding and information dominance also enhances the friendly network's ability to adapt to emerging trends in the OE. While elaborate communication architectures have been developed to facilitate information sharing and database access, the challenge is to ensure information is correctly classified and communicated to the necessary entities while avoiding information overload in order to find the relevant, useable information that supports decision making. Ensuring a comprehensive approach requires "need to share" and "write-for-release" mind-sets and appropriate policy together with active communication through all levels of Alliance organizations, relevant international entities (e.g. United Nations,

⁵ PO(2011)0045 Updated list of tasks for the implementation of the Comprehensive Approach action plan and the Lisbon summit decisions on the Comprehensive Approach, 1 March 2011

international Law Enforcement, Non-Governmental Organizations, etc.), as well as all elements of Alliance Nations' elements of power (Diplomatic, Informational, Military, and Economic). This paradigm shift in Alliance information-sharing policy and practice is necessary to deny threat and other malign networks the freedom of action and manoeuvre they need to exploit between the policy boundaries and cultural divides of these friendly entities and organizations. The following are key:

- (1) *Collaboration*. Collaboration is key to AtN/CTN activities. It enhances planning and execution, intelligence collection, analysis, reporting and targeting. Collaboration includes:
 - (a) *Military-Civil Collaboration during Planning and Execution*. A comprehensive approach to cooperation (Including Coalition, NGO, WOG, etc.) that facilitates and encourages situational awareness (What Information is Available) and synergy is necessary. All participating military and civil organizations should be integrated into AtN/CTN planning to develop a shared understanding of their priorities and capabilities. They should also be included in execution. Inclusion of Host Nation security forces in COIN operations, for example, demonstrates the competency of the security force and effectively increases their legitimacy in the eyes of the populace. Developing an effective collaborative environment requires the joint force to engage HN partners and civil organization partners and to share information. This effort is even more critical if and when the military is assisting lead civilian and international organizations in CTN outside of a JOA. A methodology for attaining this level of cooperative exchange includes:
 - i. Establish communications (face-to-face meetings are preferred along with the exchange of liaison officers).
 - ii. Determine missions, tasks and mutual goals. Identify and discuss points of divergence.
 - iii. Determine and discuss the information requirements that support these missions/tasks. Identify the specific types of information that needs to be exchanged to facilitate mutually supporting operations and the timelines for providing that information to decision makers and planners.

iv. Discuss methods for establishing communication architecture for on-going information exchange. Challenges to communication might be extensive, given differences of culture, language and technologies.

v. Determine respective meeting schedules and battle rhythms and decide when/where to meet. Liaison officers should attend and participate in appropriate meetings.

(b) *Intelligence Collaboration.* AtN/CTN activities are inherently dynamic and involve fleeting targets with short windows of opportunity for exploitation. In order to work, the system requires detailed and continuous coordination between collectors and customers throughout the entire comprehensive approach. Also, we need to think beyond traditional military intelligence in AtN/CTN and include criminal intelligence, forensics, and financial intelligence data to be effective against these malign networks.

(c) *Communications Architecture.* The Alliance must establish a flexible and responsive communications architecture within the Joint Force that supports operations by facilitating the exchange of relevant intelligence and appropriate information among all the AtN/CTN participants

(d) *Collaborative Targeting.* Establishing a collaborative and flexible targeting process is critical because it provides current unit troop to task assessments of the operational area, and allows for the exchange of information in real time. This decreases the time required to plan and execute operations and speeds up decision making. Collaboration must occur not only vertically between the echelons (joint force to components to manoeuvre units), but also horizontally across staff sections and the HN's security forces. However, the technological capabilities of all partners is not consistent, so the Alliance must provide a common information sharing framework as well as enable a non-technical information sharing capacity. Moreover, since the Joint Force must understand and support a new paradigm for CTN Targeting in the AI against transnational threat networks that includes non-kinetic applications such as arrests, financial seizures, sanctions, demarches, and even informational and defensive cyber countermeasures.

(2) *Knowledge Sharing.* Alliance, as well as National forces, have multiple high-speed networks, video teleconferencing, digital mapping, satellites, and significant amounts of high-tech equipment designed to make information instantly available to those who need it. However, the adversary networks also have a highly adaptable communications network utilizing cell phones, video cameras, Internet access, e-mail and messengers. The goal of a knowledge sharing process is to create, facilitate and manage a horizontally based, vertically integrated knowledge transfer system which is designed to harness emerging threat and friendly information that is rapid and flexible. This creates a competitive advantage against a networked threat through technological innovation, cultural engagement, and proactive coordination. While most Alliance commands designate a knowledge management officer (KMO) who works with the communications staff and representatives from the intelligence and operations staff to craft the command's knowledge sharing processes, effective information exchange cannot be based solely upon a technology based process critical to AtN/CTN is to ensure that relevant information is delivered to the right person at the right time through the entire levels of conflict (tactical through strategic). A good example of this knowledge sharing ethic is the application of the "Jones Principles of Information Exchange"⁶:

- (a) Focus & Flexibility.
- (b) Simplicity & Pragmatism (Economy of Effort)
- (c) Agility & Releaseability

(3) *Employ All Enablers.* To conduct effective AtN/CTN, it may be necessary to augment the Joint Force and select unit level headquarters with teams of specialists (e.g., analysts and subject matter experts (SMEs) such as law enforcement, weapons technicians, human environment teams, snipers, Psy Ops experts, CIMIC personnel etc). These enablers provide niche intelligence collection and analytical abilities, not normally resident in the Joint Force, to maximize the Joint Force's capabilities. Inclusion in the staff and the targeting process allows the enablers to understand the context of the operation, visualize the commander's intent and provide the best advice and support to the commanders and staff

Jones Principles for Effective Information Sharing presented at the 2011 NATO C-IED Conference by Maj Jason Jones, NZ Army.

members. Additionally, fully integrated enablers are able to serve as advocates for support requests to parent and supporting organizations through direct communication or intelligence reach-back. Suitable tasks would be to:

- (a) Facilitate the gathering, interpretation, and processing of information.
- (b) Assist in understanding the OE (i.e., culture, religion, and politics).
- (c) Report and collect signatures to provide trends, TTPs, and predictive analysis.
- (d) Assist and support in the targeting and engagement process.

Influence Neutral Networks & Exploit All Opportunities with Information Operations (IO)

5. As previously stated, AtN/CTN requires the application of a mix of lethal and non-lethal means to successfully neutralize the threat network. It also requires a well-crafted influence campaign to win-over, or prevent the adversary from winning-over, the neutral, or “fence-sitting” population of individuals and networks. This applies not only in the AO but also in the AI. This maximizes friendly network support and/or minimizes additional threat networks support. While targeting threat networks, lethal means are often emphasized within the JOA, but in the long term, non-lethal options, led by effective IO, have a greater cumulative effect, especially when it comes to turning the local population against the enemy. For most threat networks, experience in the past 10 years of conflict has shown that eliminating key individuals has only a limited disruptive effect; individuals are quickly replaced. Alternatively, effective IO has enduring effects in setting conditions (shaping), exploiting mission success, and mitigating the effects of negative events. Planners must design an agile and flexible IO plan that can quickly respond to dynamic situational developments and that target appropriate audiences. The basic premise being *“the truth counters enemy propaganda and reduces their local population support.”* IO must shape all operations by assisting to secure the populace, explain the operational rationale, and demonstrate the results of the operation as well as counter threat propaganda and inherent cultural misperceptions. With that said, lethal and other kinetic operations do still have a role in AtN/CTN, but must be synchronized with non-lethal/non-kinetic activities vice the more traditional roles of either a segregated IO campaign or the IO campaign supporting the kinetic efforts.

6. Initially, the detailed JIPOE will identify those societal elements (leaders and general population groups and subgroups) whose support, or neutrality, will be the focus of friendly IO. JIPOE will also determine the interests and objectives of those individuals and groups (See Figure 5) that can be the basis for developing themes. Synchronized, integrated, multi-level IO is critical to AtN/CTN because it can help shape the OE, multiply the effect of friendly success, mitigate negative actions, and counter enemy propaganda. IO can also directly affect the perceptions of the threat network leadership.

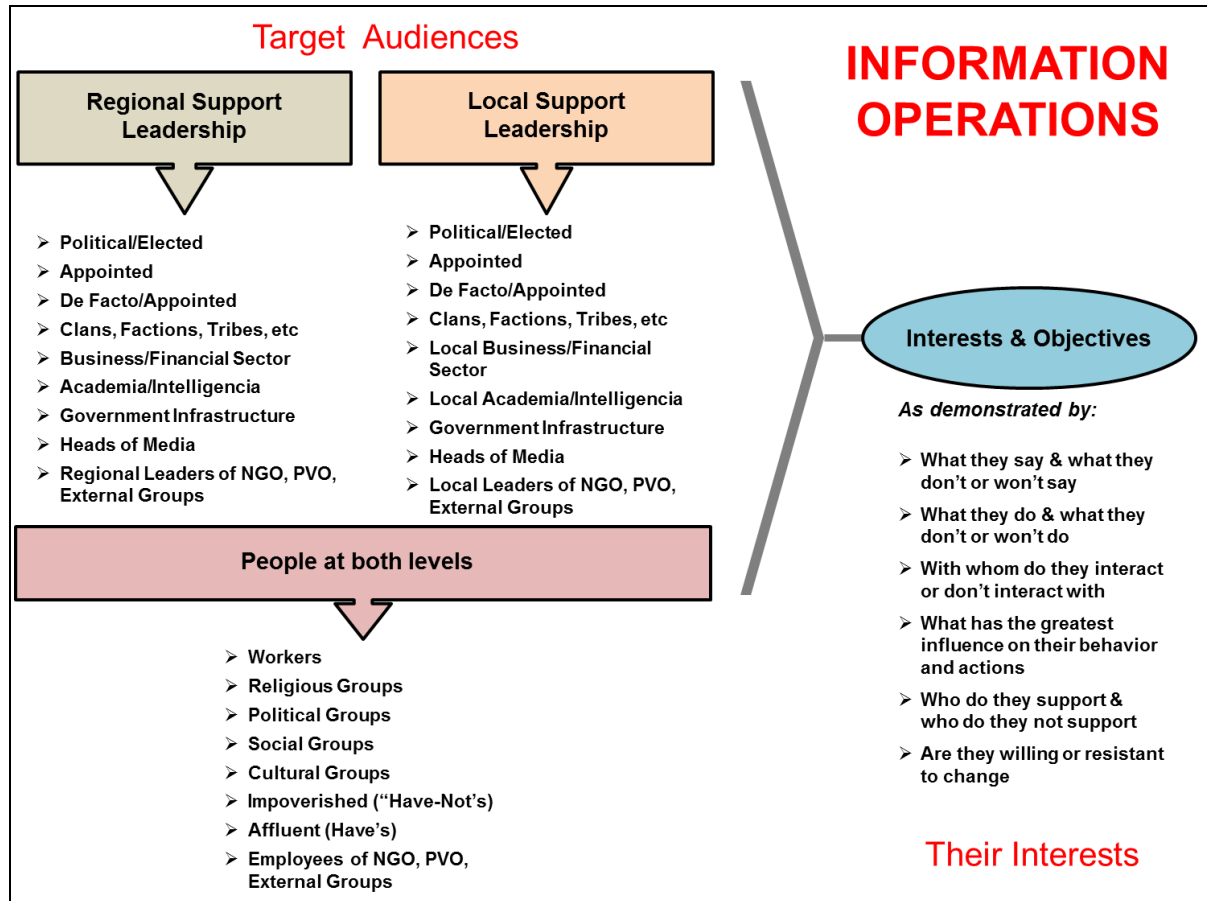


Figure 5 - IO Audiences and Interests

7. Effective IO will do the following:

a. *Setting Conditions.* The principle of isolating adversaries from their cause and support requires changing environmental conditions within and beyond the boundaries of the engagement area. IO provides a potential mechanism for shaping or changing the environment that supports continued enemy activity by attacking the legitimacy of their actions. IO can be used to positively (reward) or negatively (punish) influence the target audience. Additionally, information

products can be developed to support an environment of improving conditions as a result of visible security measures taking place in the area. The products provide a mechanism for engagement with the population and are distributed while active (usually offensive) operations are conducted to reduce the engagement area. In setting conditions, the friendly force at all echelons should conduct a series of Key Leader Engagements (KLE) to provide local leaders with information on upcoming operations and how they will affect and improve security in the operational area. For example, in COIN operations, engagement can be conducted with local shop owners and businessmen in the area to explain actions underway and solicit support in reducing violence in the area. These interactions set conditions by managing the expectations of local leaders and population and assist in illustrating the positive actions the government and security forces are taking to secure their safety.

b. *Shaping*. Once conditions are set in the targeted area, unit IO staffs will participate in execution. This can take a number of forms depending on the unit capabilities and the type of IO activities the Joint Force is executing.

8. IO does not terminate with the conclusion of the combat phase of a joint operation. Post-combat IO is equally important. It continues well beyond the end of the combat in order to exploit success or mitigate negative consequences. The joint operation and subordinate plans must ensure that post-combat IO is appropriately planned, prepared and resourced. Options include the IO staff preparing messages for the friendly force leadership (Alliance, national, & HN security forces) to deliver at press events or through interaction with local leaders in the immediately affected area and throughout the operational area. IO analysis teams perform continuous assessments to determine the population's view of the operation and how it impacted their situation. This can include something as simple as claims forms for damaged property. Additionally, the Joint force can employ intelligence resources focused on the enemy's reactions to include determining how they rebuild their capacity and take other steps as necessary.

Interdict, Neutralize, Isolate and Exploit Threat Networks

9. Networks operate in inherently complex environments that are often difficult to understand and which often defy coherent joint operation planning. As a result, identifying the opportunities that can be exploited in threat networks is often challenging and requires detailed analysis based upon a well-founded understanding of the OE. This is specifically in relation to the interrelation of the Political, Military, Economic, Social, Infrastructure, Informational (PMESII) and it is critical to understanding threat networks in order to conduct an effective Critical Factors Analysis (CFA)/Centre of Gravity (COG) Analysis. The essential CFA outcomes will also assist in identifying the

centre(s) of gravity and decisive points based upon nodes and links discovered in the networks. This will help focus the employment of intelligence resources on identifiable threat activities and help prioritize potential targets for lethal or non-lethal exploitation during operational activities. While AtN/CTN planning activities, nested within the broader OPP and its supporting activities, are normally not conducted independently, this PMESII-based CFA is the critical difference between major conventional operations- based Intelligence Preparation of the Battlespace (IPB).

10. Successful AtN/CTN planning and execution normally is accomplished by working with Alliance, international, and HN partners to conduct a complimentary and coordinated mix of lethal and non-lethal actions (discussed in detail in Chapter IV) focused on specific nodes and links in the threat network. Successful AtN/CTN operations will blend actions that directly degrade/interdict threat network capabilities and that shape and influence neutral networks, all the while increasing friendly network capabilities. These actions span the spectrum of conflict and include general purpose forces and special operations forces, as well as specialist and non-military capabilities (e.g. counter threat finance, law enforcement actions, etc). Although it is likely that the threat network will never totally disappear, it is considered to be neutralized when its capabilities are marginalized or sufficiently interdicted or degraded and where friendly network capabilities have improved to the point where they can manage any residual threat independently over time.

11. The AtN/CTN activities described in this handbook primarily apply to joint operations that do not involve adversary state-sponsored, conventional military forces, but even traditional nation states are leveraging the asymmetric capabilities involving threat networks to act as proxies. While AtN/CTN is most applicable to threat networks during counterterrorism, stability and counterinsurgency operations, it can also be applied to a wide variety of irregular, networked threats (transnational criminal organizations, terrorists, piracy, etc.) that threaten Alliance interests or those of our partner nations. Also, NATO military organizations do have a significant role to play in supporting civilian led CTN efforts outside the JOA with information and intelligence sharing as well as assisting in the coordination of countermeasures against transnational threat networks.

CHAPTER III

UNDERSTANDING ADAPTIVE THREAT NETWORKS

Introduction

1. Understanding the threat network requires a basic appreciation of the nature of adaptive networks; their structure and components, characteristics, attributes, and purpose. Although different from conventional military threats, once these differences are understood, the analytical process for describing the threat network and predicting its behaviour remains largely the same.
2. Pattern analysis, link analysis, social network analysis, and forensics are the foundational analytic methods that enable intelligence analysts to create a template of the threat network, focusing ISTAR capabilities, and providing intelligence support to targeting. Available intelligence is fused and simplified to create a model of how the threat network generally operates. This activity model can be further refined into a narrative and graphic template of the network. The network activity model and the graphic template support critical factors analysis, which is a detailed functional breakdown of the network activities to identify its critical capabilities, requirements, and vulnerabilities.
3. Networks are increasingly defined using the following lexicon:
 - a. *Network* - That group of elements forming a unified whole, also known as a system.
 - b. *Cell* – A subordinate organization formed around a specific process, capability or activity within a designated larger organization (a cell can be a network unto itself or an element of a larger network - i.e. the finance cell).
 - c. *Node* - An element of a network/system that represents a person, place, or physical thing.
 - d. *Link* – A behavioural, physical, or functional relationship between nodes.
 - e. *Actors* – All parties and stakeholders that are part of the operational environment and who either directly or indirectly have a share, take part, or influence, the outcome. (AJP-3.4.4; a proposed new term and definition)

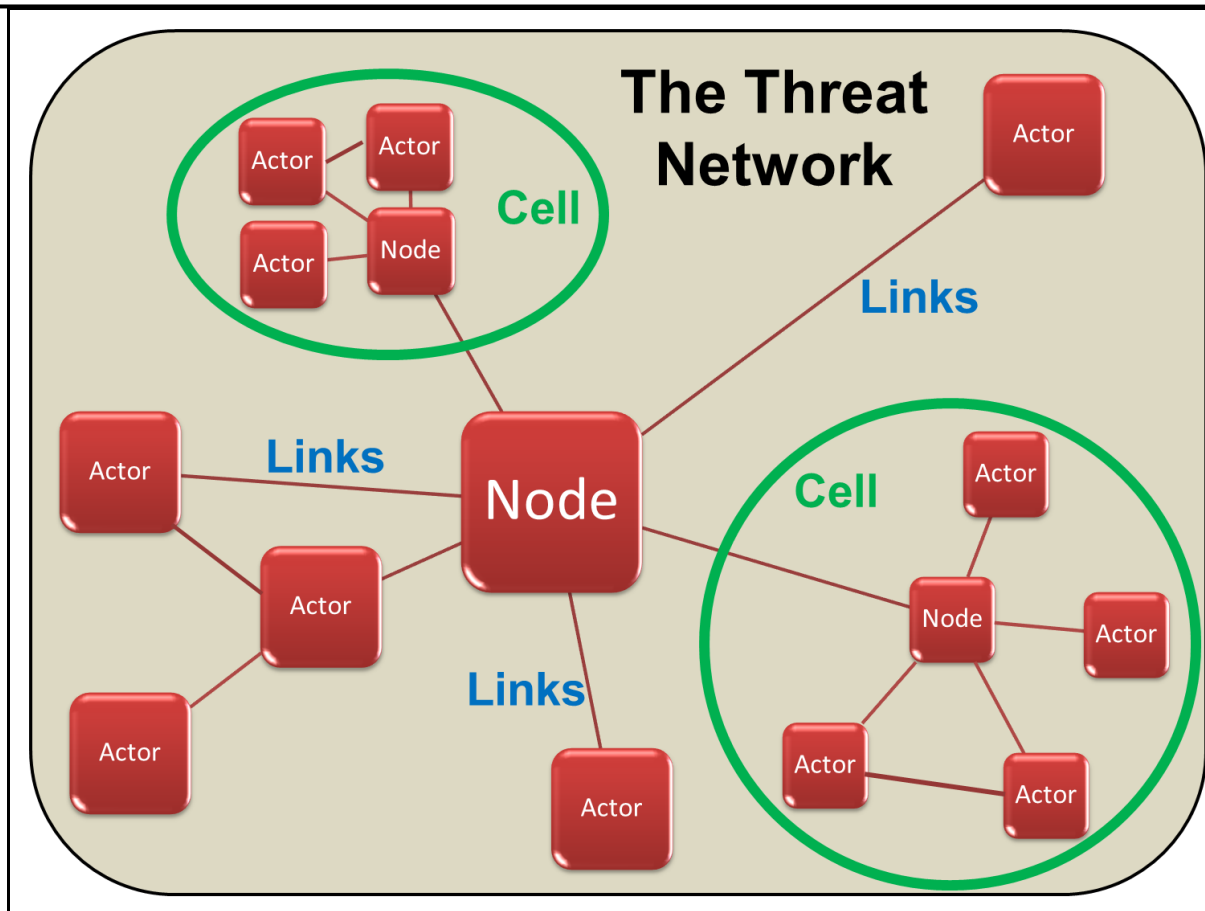


Figure 6 - Typical Structure of a Threat Network

Threat Network Characteristics

4. Some typical network characteristics are:
 - a. *Types and Components.* There are many types of networks – insurgent, criminal, social, or conventional military networks (e.g., computer, air defence etc.). While they take many forms, networks are basically comprised of people, processes, places, and material – components that are identifiable, targetable, and exploitable.
 - b. *Forms and Purposes.* Networks vary in basing, size, shape, membership, cohesion, and purpose. Successful networks are well integrated into their operating environment and so they are hard to locate and even harder to effectively attack. Some networks are territorially based, such as the FARC in Colombia, while others have little physical presence in their target countries and their members are spread across the globe. Transnational networks make full

use of the interconnected global environment to direct operations, raise money, obtain and train recruits, and freely exchange technological information. Globally dispersed cells working autonomously towards the network leadership's endstate provides a degree of safety to the cell; once a successful technique is perfected it can quickly be spread to other cells globally through internet or social media. A specific network can be narrowly and tightly focused on one goal or more broadly oriented toward many goals. It can be either exclusive or encompassing in its membership. For example, a human network is an alliance of socially connected individuals who are involved in activities to achieve some form of social, political, monetary, religious, or personal common goal.

c. *Attributes.* In order for the network to survive in an environment while being hunted, the enemy must continuously respond to changing environmental pressures, including political, economic, social, and military factors. Survival and success are directly connected to the network's adaptability and ability to compete for resources – financial, logistic, and human. While threat networks possess many attributes, among the ones important to their success are:

- (1) *A flexible command and control (C2) structure.* Some networks are flat and decentralized while others are centralized and hierarchical and some are a mixture of both systems, but they are all designed to facilitate the attainment of the network's goals and its continued survival.
- (2) *Shared identity.* The membership is often based on kinship, ideology, religion and personal relations. This helps to bond the network and also facilitates recruitment.
- (3) *Competency.* Knowledge, skills, and abilities of group leaders and members.
- (4) *Resources.* An essential attribute in the form of arms, money, social connectivity, and public recognition.
- (5) *Adaptability.* This includes the ability to learn and adjust behaviours and to modify TTP in response to friendly initiatives.
- (6) *Sanctuary.* A safe haven allowing the conduct of planning, training, and logistic reconstitution.

Network Strengths and Weaknesses

5. The *strength* of a network revolves around the following factors. Typically, they have:
- a. *The ability to adapt over time.* This is a fundamental requirement for any network to survive.
 - b. *The ability to blend into the OE.* This can make it difficult to separate the enemy from the local population. Many of these networks are also transnational making them significantly more difficult to counter.
 - c. *The ability to rapidly replace personnel.* Any losses on lower levels in the network can be quickly replaced by recruiting new members, usually through personal relationships.
 - d. *A measure of insularity.* The relative insularity of threat networks can make it difficult to gain intelligence about them and their activities. This impenetrability is based primarily on the bonds of kinship, religion, and purpose that tie members together.
 - e. *The ability to establish a cellular organization with certain levels of security due to clandestine and covert actions.* This factor limits the friendly force's ability to roll up sizable portions of the network, at any one time.
 - f. *The ability to make multiple connections.* Networks can be highly connected both internally in terms of their members and externally to the respective country's cultural and social structure. Individuals can be connected to one another and to their leaders in multiple ways. This includes kinship, religion, former association and history, among other factors. This layering of affinity creates dense, internally connected networks and supports their cohesiveness. Through their membership, these networks are also connected to major social structures like the tribal system and/or a religious structure. This gives networks the opportunities to acquire both resources and support.
6. While threat networks have inherent strengths, they also have exploitable inherent *weaknesses*. These may include:
- a. *Competition for resources.* This may be in terms of combat supplies, recruits, IED manufacturing materials, finances or even the loyalty of the population. This often leads to one group working against the other. Such conflicts of interest, and their associated behaviours and deeds can open them up to detection.

- b. *Connectivity among cells.* Although the clandestine cellular structure is a highly secure one, the links between cells can be identified and exploited over time since communications between cells and leadership is often a critical vulnerability and frequent necessity. Putting pressure on one cell, can lead them to try to gain support from another and thus help more links and connections to be detected, identified and exploited.
- c. *The need to “surface” to take action.* When a cell has to interact more with the population around it and with its environment, it opens itself up to detection. This is especially true during the preparation, planning and reconnaissance phases prior to an attack. This can expose some cells and key network functions to interdiction and attack.
- d. *Their natural tendency to replicate previous successful actions.* Competition for resources, previous positive propaganda, preservation of capability, and seeking short term recuperation by slowing down the battle pace can all be reasons for this tendency. In effect it leads them to set patterns and follow predictable TTP. These are all factors which can be identified and exploited.
- e. Internal fracture in threat networks offers evident movements within them. Any minor modification or biased perception of the shared identity from the internal perspective, use to create strong changes of trends in the threat networks activities. These change points are easy to be detected and offers new targeting possibilities.

Identifying and Defining a Network

7. There are various analytical processes, often working collectively, that can help to identify and define a network. These are:

- a. *Macro Analysis.* To develop a threat network profile, the staff need to first identify the network that poses the greatest threat. For example, in a COIN environment where population protection is paramount, insurgents attacking the populace might be a higher priority than those merely attacking friendly forces. Consequently, friendly forces analyse and exploit threat network tactics, techniques, and procedures. They determine which threat network poses the highest threat. Once the network is identified, a more detailed analysis is conducted with the help of specialized resources (such as national reach-back capability or other enablers). This initial macro analysis seeks to identify threat network critical capabilities, requirements, activities, and operational areas and then, using CFA (detailed below), its critical vulnerabilities. This enables the staff to identify potential targets and the target area. During macro analysis, analysts

will assist the staff in determining which nodes, or links, of the targeted network can be identified with actionable intelligence and which of those network nodes and links represent the most lucrative targets for achieving the desired effects.

b. *Critical Factors Analysis (CFA)*. This is a holistic approach to understanding the critical capabilities and requirements of a particular network's operations. It assists commanders and their staff in identifying the critical vulnerabilities, and points of exploitation, for lethal and non-lethal attack. In order to continue to exist, a mature network usually possesses certain baseline critical capabilities and requirements to ensure the network functions. Many of these can be subject to discovery and exploitation, thereby becoming critical vulnerabilities.

c. *Activities Analysis*. Networks have to be active in order to exist and function. While the baseline critical capabilities and requirements are common to all networks, the specific activities that they regularly engage in will vary depending on the type of network. However, *it is worth noting that many IED network tasks are shared with activities that are supporting other insurgent, terrorist, and criminal behaviours such as drug trafficking, human or commodity smuggling and money laundering*. Often, through detecting, tracking, and exploiting general "pattern of life" activities, NATO forces can identify how a network is structured, sustained and conducts its operations. Networks enhance their survivability by carrying out many of their supporting tasks on an independent, simultaneous basis. Participants in each function may be completely unaware of the others existence. This limits the network's vulnerability to a handful of key personnel who are orchestrating the network's overall activities. Not all network activities are critical, but information derived from non-critical activities can lead to the identification and exploitation of vulnerabilities.

d. *Micro Analysis*. Once the initial macro analysis is accomplished, the staff and supporting analysts can then produce micro network data by leveraging all source information (to include information derived from the exploitation of enemy activities). This effort includes:

- (1) *Synchronizing specialized analytical assets with ISTAR capabilities and with reach-back to national-based resources*. This enables the production of practical, useable intelligence against threat network personnel, functions and activities in order to find additional actionable targets. The Joint Force staff analyses adversaries in named areas of interest (NAI) and identifies patterns of enemy activity in order to mass ISTAR assets on the NAIs for extended periods. Massing ISTAR assets further refines targetable data and facilitates the attack of multiple

network targets with near simultaneous multi-echelon operations. As an operational technique, the Joint Force can conduct a series of small-scale shaping operations to cause the threat network to react through increased communications and movement of personnel. These activities can be carefully monitored by Signals Intelligence (SIGINT), Human Intelligence (HUMINT), and Ground Moving Target Indicator (GMTI) radar to gain additional information. Once sufficient actionable intelligence has been developed, operations will be conducted, the results exploited, and follow-on missions conducted as required.

(2) *Creating network templates.* This activity allows analysts to graphically represent those functions and activities, overlaying what we know and what we don't know, in order to refocus Priority Intelligence Requirements (PIR) and create opportunities for learning. Network templates enable the commander and staff to map the network's people and activities on the ground, using all-source intelligence, in order to "fix" the target network. A basic template identifies potential High Value Individuals (HVI), NAI, Target Areas of Interest (TAI), detailed processes, and how we can detect them through the development of indicators (observables and signatures). This is the "what we know" part. The "what we don't know" part promotes PIR refinement which is then used to identify and optimize AtN/CTN collection gaps, to focus collection on already known NAI, HVI, and processes, as well as collection to expand the "what we know" part of the puzzle.

f. *Analytical Methodologies.* When analysing a threat network, it is useful to ask some basic questions that assist in understanding how the network functions and the complexities of the relationships between and among its critical capabilities and requirements. Answering these questions can often reveal potential critical vulnerabilities that can be exploited by lethal and non-lethal means. There are a number of analytical methodologies that can be used to build detailed knowledge of a network's interpersonal dynamics and to do so within the context of an active operational environment. While some of these methodologies are designed to focus on specific types of networks (insurgencies, terrorists, etc.), most can be easily modified to apply to any type of network the joint force may encounter. These methodologies include:

(1) *Social Network Analysis (SNA).* This is a tool, together with its sub set, Link Analysis, that enables an understanding of the organizational dynamics of an insurgency and how best to attack or exploit it. Rather than assuming that killing or capturing the leader will achieve desired

effects upon a network, SNA helps to identify which members of the network can be killed, captured or influenced to achieve desired effects. SNA shows how an insurgent's networked organization behaves, how its connectivity affects its behaviour, where the influence resides and how it is distributed among members. However, there is a significant caveat when using SNA and that is that the link analysis is unique to the analyst developing the picture of the network. Additionally, in developing a link analysis it is critical to ensure that there is an understanding of how or why a link was made between two actors or nodes.

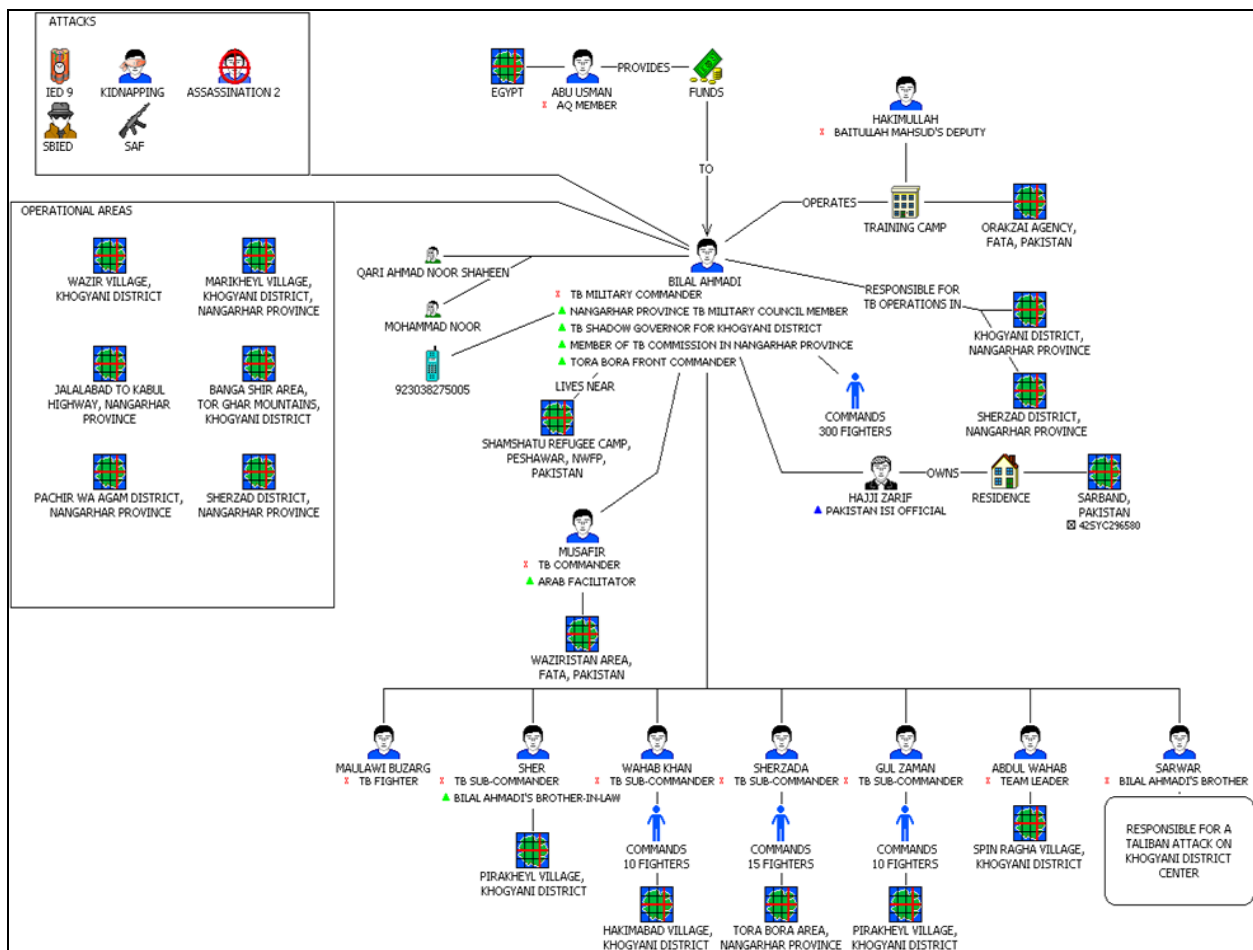


Figure 7 – Example: Typical Social Network Analysis

(2) *Association Matrix Analysis.* An association matrix portrays the existence of an association, known or suspected, between individuals, the

“who”. Direct connections include face-to-face meetings and telephone conversations. Analysts can use association matrices to identify those personalities and associations needing a more in-depth analysis to determine the degree of relationship, contact, or knowledge between individuals.

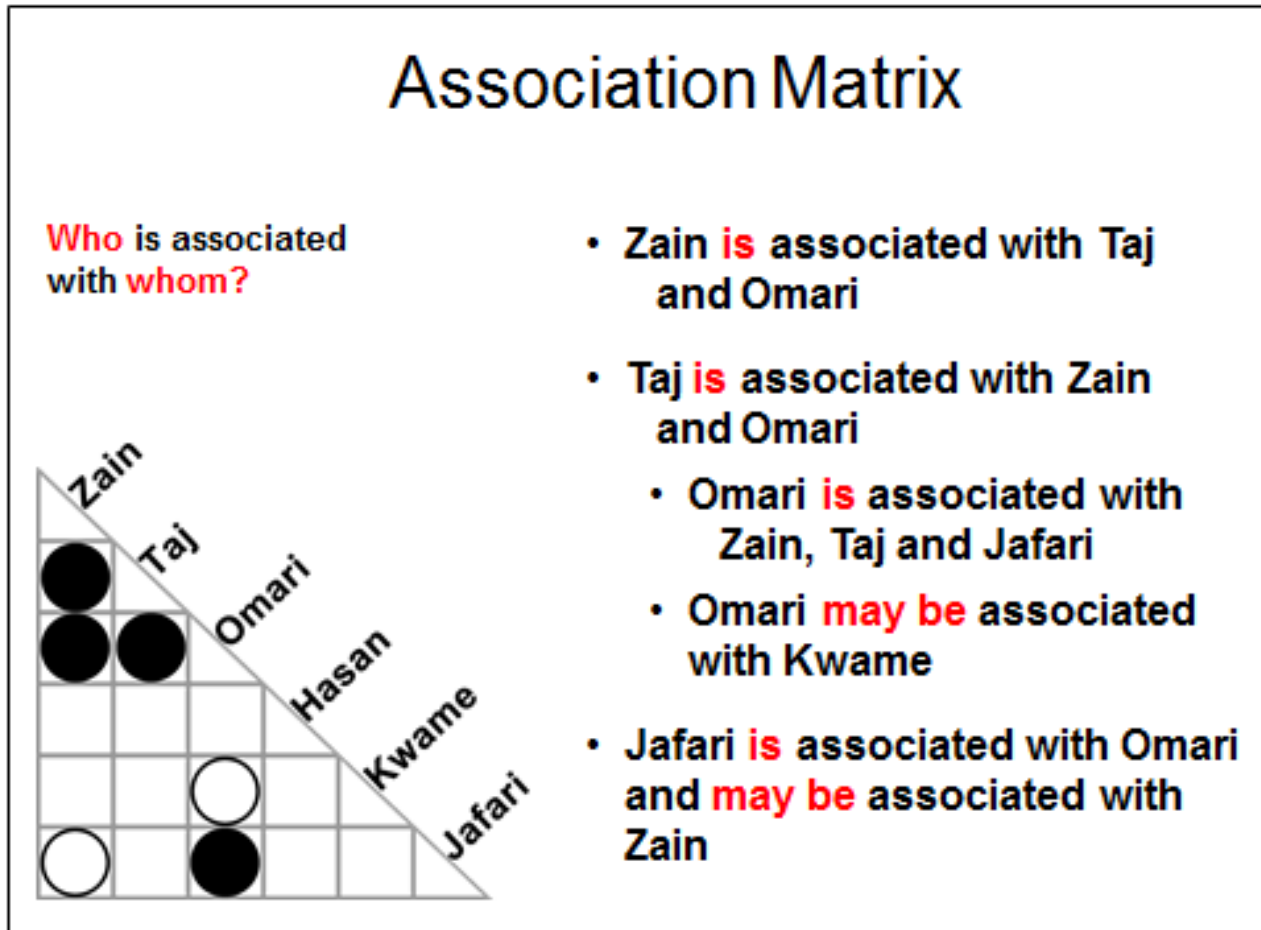


Figure 8 - Example: Typical Simple Association Matrix

(3) *Activities Matrix Analysis*. Relationships in large data sets are established by similarities between the nodes. People are identified by their participation in independent activities, the “what”.

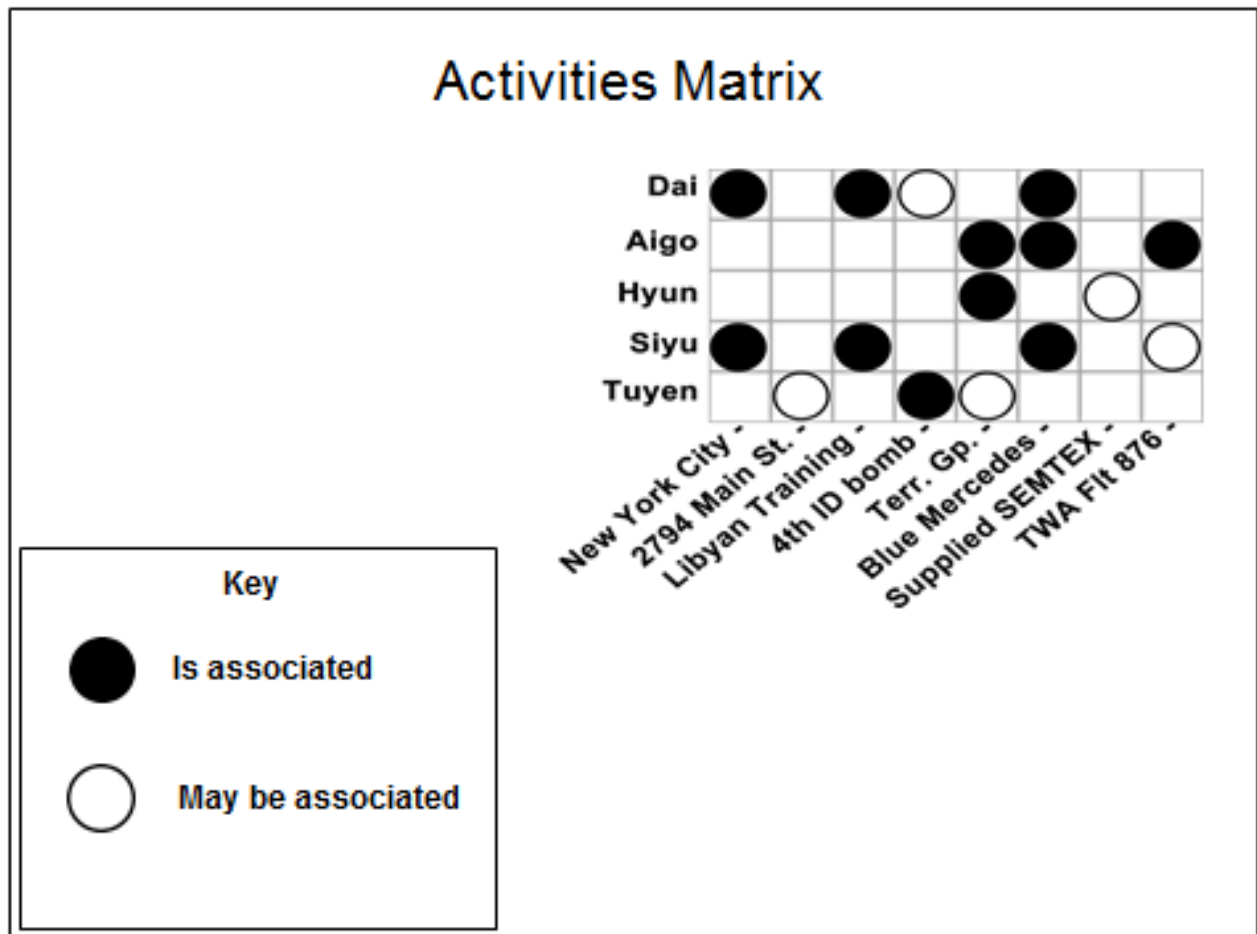


Figure 9 - Example: Typical Simple Activities Matrix

(4) *Coordinates Register Analysis.* The Coordinates Register is a pattern analysis tool and is also known as an incident map. Analysts may use multiple coordinate registers with each focusing on an individual subject or blend of subjects. It focuses on the “where” of an event. Using coordinates could be exploited more if similarities and differences of incident are made visual on a map to extract more patterns.

COORDINATES PLOTTING

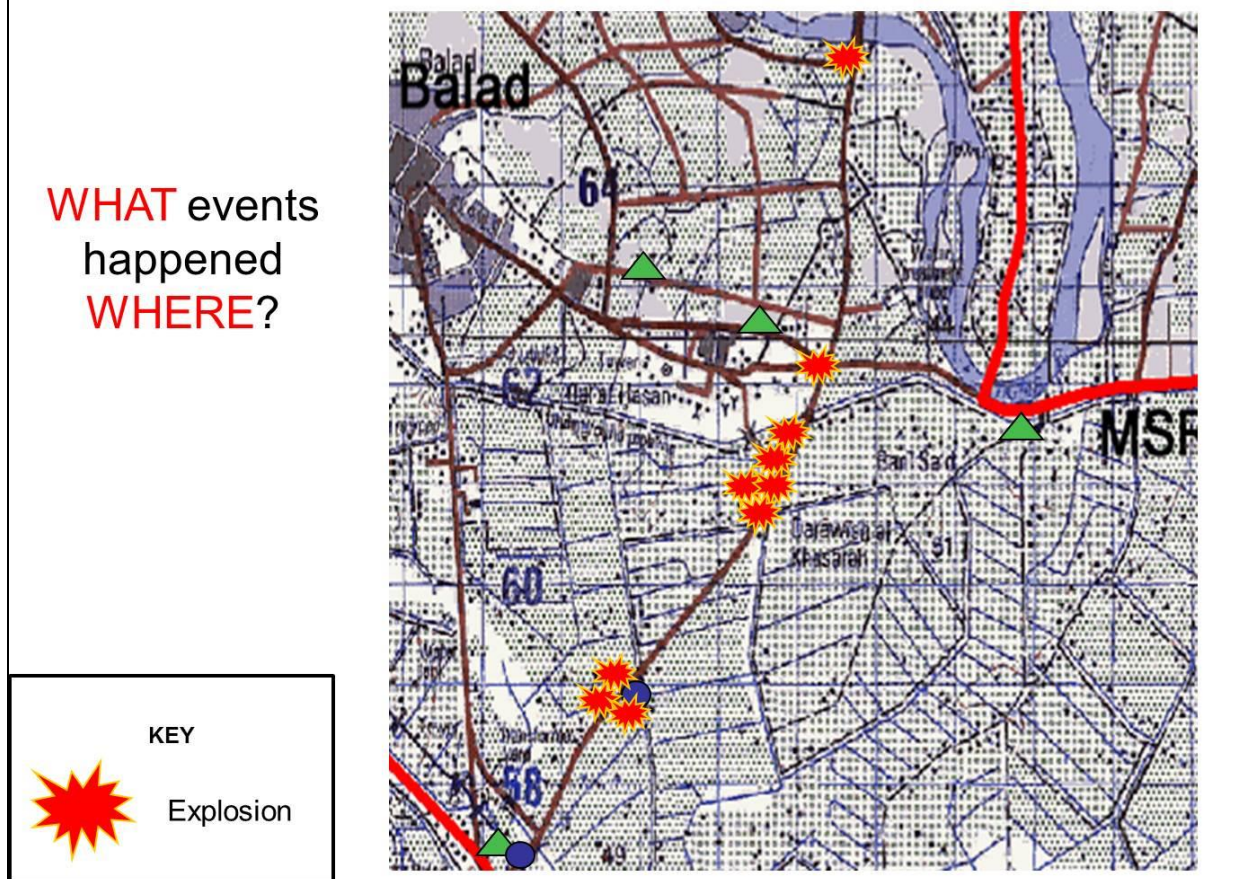


Figure 10 - Example: Coordinates Plotting Chart

(5) *Pattern Analysis Plot Sheet.* Pattern analysis plot sheets focus on the time and date, the “when”, of each serious incident that takes place within the area of operations. When used in conjunction with the Coordinates Register and other templates, the plot sheet supplies most of the data needed for an event template.

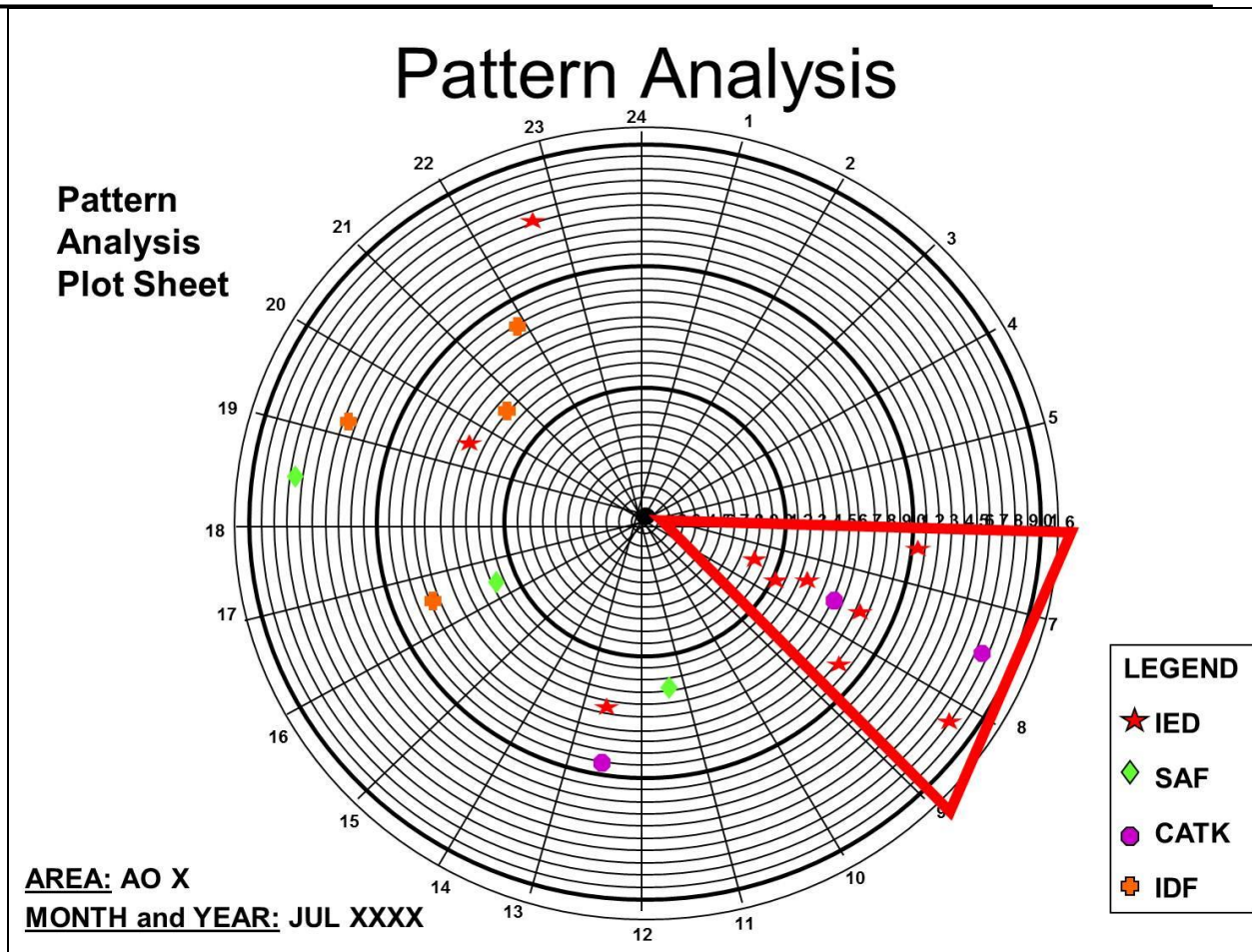


Figure 11 - Example: Pattern Analysis Chart

(6) *Time Event Chart Analysis.* Time event charts are chronological records of individual or group activities. They are designed to store and display large amounts of information in a small space. Analysts can use time event charts to help analyse larger scale patterns of such things as activities and relationships.

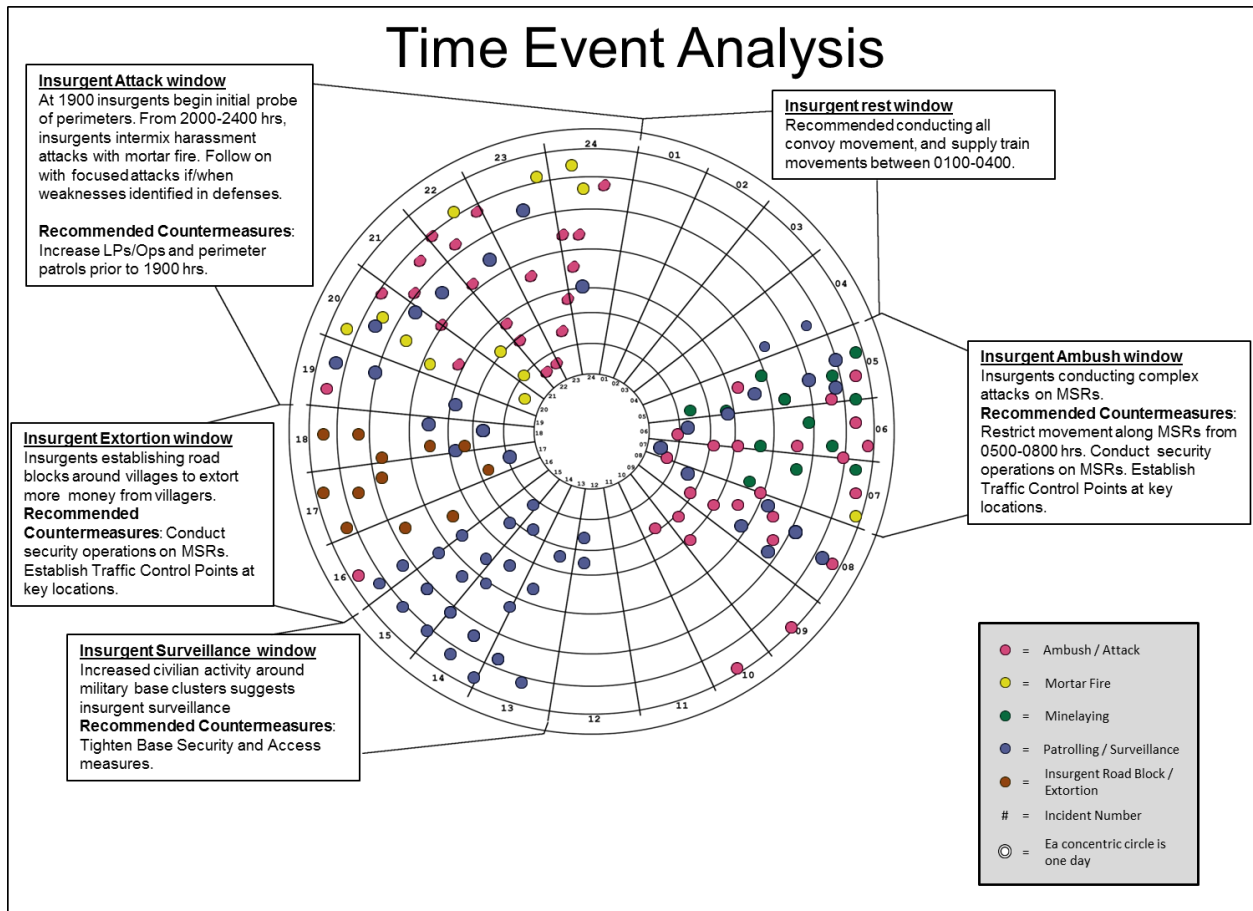


Figure 12 - Example: Time Event Analysis Chart

(7) *Nodal Analysis.* Vulnerable nodes can be identified using social network and dynamic network analysis techniques. Nodal analysis focuses on the activities that the network needs to do with the aim of determining critical nodes and the most effective way to influence that node. Nodal analysis examines the interaction and interrelationships among multiple target systems to determine the degree and points of interdependence and the linkages of their activities. Nodal analysis takes time. Nodal analysis is also complemented by individual component analysis which focuses on activity taking place within a specific node in a limited geographic area. Individual component analysis relies on perishable unit level tactical reporting and is designed to support local operations. There is also nodal component analysis which examines how nodes in a system function in relation to one another and which should lead to the identification of the critical nodes which are those nodes whose

disruption or destruction immediately degrades the ability of a network force to command, control, or effectively conduct its operations. Nodal component analysis will often use models to graphically display the system. Nodal analysis results in the identification of the specific functional nodes that empower that network. Once these nodes are identified, the next step is to develop detailed information on the specific activities that take place within that node. Such activities are generally observable and can be influenced or interdicted by lethal and non-lethal means.

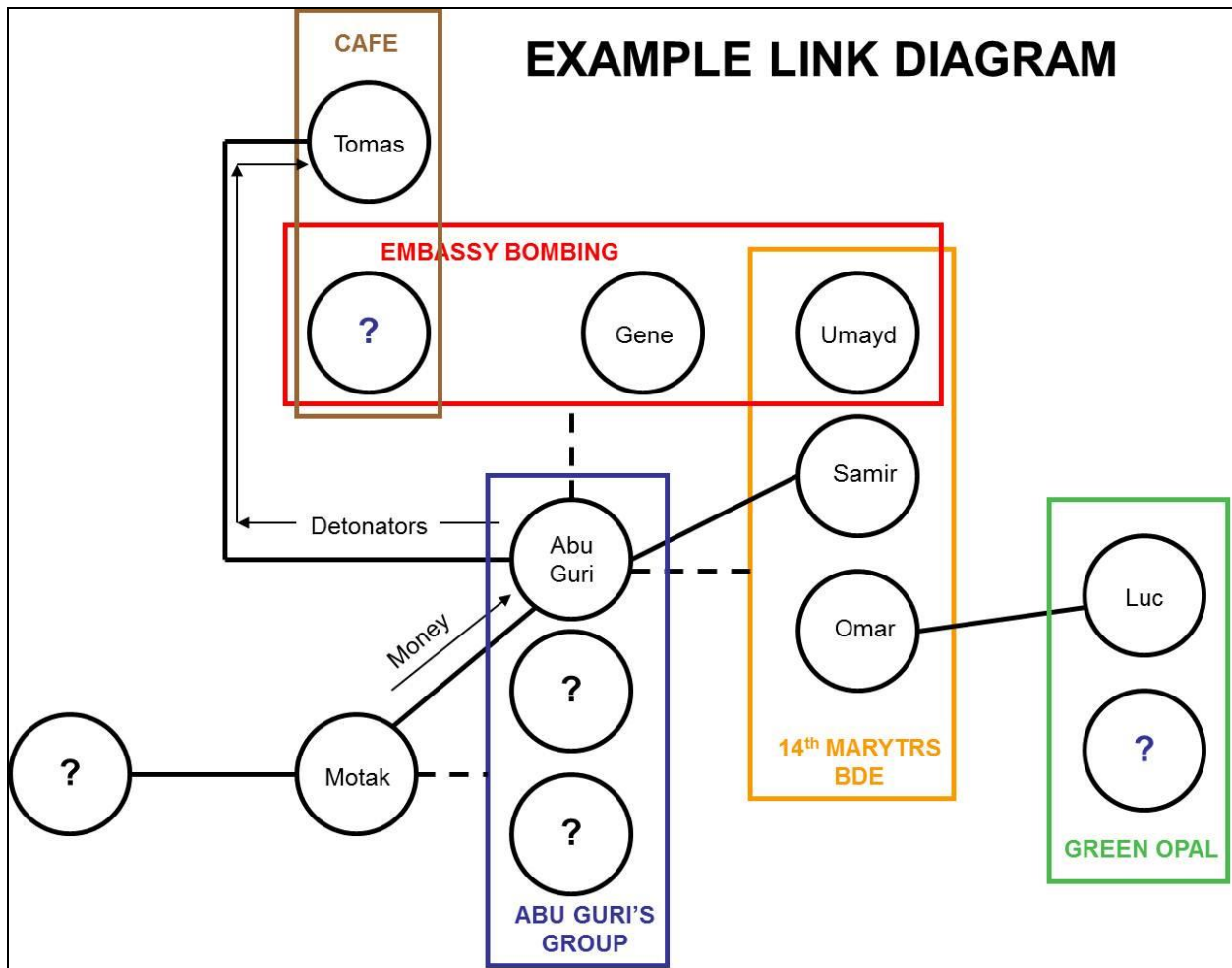


Figure 13 - Example: Link Diagram

Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR)

8. ISTAR assets are employed to gain greater situational awareness and fill intelligence gaps regarding the threat network. ISTAR supports AtN/CTN by tracking key or vulnerable nodes within a network. Employing all ISTAR capabilities (air and ground, manned and unmanned, tactical through theatre, as well as national technical means) to answer priority intelligence requirements (PIR) has a synergistic effect. However, AtN/CTN related ISTAR operations are conducted in a blended environment (where the network exists and operates throughout the operational area and beyond) and finding a low signature target can be a difficult problem. Attempting to employ limited ISTAR assets without a specific focus leads to analysis overload. Thus, when planning ISTAR support to AtN/CTN, a detailed preliminary PMESII analysis of the network's structure and activity must be undertaken to provide preliminary focus (CFA) for ISTAR employment. Over time, as the picture of the network is refined, ISTAR assets can be more tightly focused in time and space. NAI are tied to PIR. Detection assets and HUMINT are applied to NAI to create TAI for exploitation. Over time, an overview of the network should be established with sufficient detail to commence targeting of individuals and activities. When conducting CTN in the AI with lead civilian agencies, a broader view of ISTAR can include forensic labs, law enforcement agencies such as EUROPOL and INTERPOL, and international financial entities such as the Financial Action Task Force (FATF).

9. Organizing and allocating ISTAR resources for AtN/CTN requires a coordinated, synchronized, and integrated effort beginning at the tactical level and often involving the use of national level resources. Intelligence personnel at all echelons must be prepared to employ traditional and non-traditional intelligence sources to build the picture of the enemy's infrastructure and share it across the joint force. A detailed and continuous JIPOE of the network and its OE will provide a:

- a. Detailed knowledge of the network's patterns of activity and related processes.
- b. Detailed knowledge of network related observables resulting from those patterns.
- c. Detailed knowledge of the network's signatures produced by the observables.
- d. Common understanding of how such signatures present themselves, in what sequence, for what duration, and in what combination. By quantifying the signatures associated with the network, collection managers at all echelons can specifically focus ISR resources to develop actionable targeting intelligence.

10. Modern technology such as unmanned surveillance assets and biometrics collection capabilities provides the Joint Force with unprecedented abilities to maintain near-constant surveillance over specific geographic areas using a wide variety of ISTAR resources. When combined with the real time imagery, from down-link provided systems, aerial surveillance assets can provide AtN/CTN analysts and targeting professionals with vital information on enemy activities. This support is also capable of detecting and tracking individuals to their safe houses and caches. Once these support sites are located, they can be further exploited to identify and locate other network functions.

11. When these enhanced visual surveillance capabilities are combined with SIGINT means and HUMINT resources (media exploitation, informers, volunteer Host/Partner Nation information sources, patrol reports, etc.), the AtN/CTN related Intel analysts and targeting professionals can develop an accurate picture of the critical nodes of the various networks working in their operational area. Gathering basic “street level” information is an essential part of AtN/CTN. Whether we are looking at individual soldiers on patrols, or information derived from meeting local leaders, or even conversations with local workers, all of these are information sources. While interactions with the local population and their observations of the physical environment may be considered a tactical concern, when aggregated, they can provide an operational level picture of enemy activities. Over time this information can be refined sufficiently to produce targetable intelligence and further opportunities for exploitation to facilitate countering the threat networks.

CHAPTER IV

COUNTERING ADAPTIVE THREAT NETWORKS

“It takes a network to defeat a network. But fashioning ourselves to counter our enemy’s network was easier said than done, especially because it took time to learn what, exactly, made a network different. As we studied, experimented, and adjusted, it became apparent that an effective network involves much more than relaying data. A true network starts with robust communications connectivity, but also leverages physical and cultural proximity, shared purpose, established decision-making processes, personal relationships, and trust. Ultimately, a network is defined by how well it allows its members to see, decide, and effectively act. But transforming a traditional military structure into a truly flexible, empowered network is a difficult process.”

General (Retired) Stanley McChrystal,
Foreign Policy,
March/April 2011

AtN/CTN Engagement Overview.

1. There are a few major differences between attacking a conventional force and attacking a threat network. The emphasis for AtN/CTN is on the employment of specialized intelligence resources and analysis to identify and define the network. This is followed by the implementation and synchronization of multi-echelon targeting mechanisms against the network. This includes employment of conventional forces, special operations forces, IO, counter threat finance activities, as well a cyber-based, computer network operations. Further, depending on the target set, small tactical units will usually be tasked with the primary responsibility for action execution; while higher echelons have the primary responsibility for planning, coordinating and allocating supporting resources.

Successfully exploiting a threat network is very difficult, especially outside of the JOA. Outside of the JOA, NATO has very limited options to disrupt networks. Network development in this environment can truly be a global endeavour that will require NATO nations to rely much more on Law Enforcement and other civilian/gov’t agencies to coordinate amongst each other and with their counterparts from other countries to develop networks and options to disrupt them.

2. As a result, Joint Force targeting efforts must employ a comprehensive approach, leveraging civil agency lethal and non-lethal capabilities synchronized with appropriate military force support that keep continuous pressure on multiple nodes and links of the network's structure. There are a few instances when specific critical capabilities and requirements may be separated from the enemy's overall operational patterns and then be subject to attack and interdiction. When conducting C-IED operations, for example, these include bomb making facilities and the bomb makers, and the acquisition of specialized components. By targeting these specific capabilities, the Joint Force may temporarily disrupt IED attacks at the tactical level, but the only effective way to counter an enemy's IED employment, in the long term, is to effectively neutralize the threat network's overall ability to operate.

Engaging and Countering Threat Networks at each Level of Conflict

4. Engaging threat networks starts with the comprehensive application of the instruments of national power of the Alliance nations (diplomatic, military, information, economic) at all levels of conflict (strategic, operational, and tactical). Additionally, the Alliance needs to coordinate with other international organizations including the United Nations and international Law Enforcement organizations (e.g. INTERPOL and EUROPOL) to ensure synergistic effects throughout the OE. The AtN/CTN activities conducted at each level of conflict must be synchronized and coordinated to ensure that the efforts are complimentary with regard to friendly plans and operations and also be cumulative with regard to the targeted threat networks.

5. At the strategic level, AtN/CTN is focused on regional/global threat networks. AtN/CTN activities may be a subset of a broader crisis response or stability operation which includes positively shaping the OE and developing and providing the partnerships, information, and resources required for strategic success. Success at this level normally depends heavily on influencing a range of audiences including local populations, threat network members and supporters, allies, and the Alliance public. Strategic actions can also be specific actions designed to gain intelligence, conduct analysis and targeting, and neutralize or eliminate nodes that are far enough outside the operational area as to be vulnerable only to a non-Joint Force agency or partner nation(s) actions. Figure 14 is an example of a multi-level approach to attacking various critical nodes in an insurgent based network employing IEDs by leveraging the multi-agency capabilities at each level of war through a mix of actions designed to achieve the desired lethal and non-lethal effects.

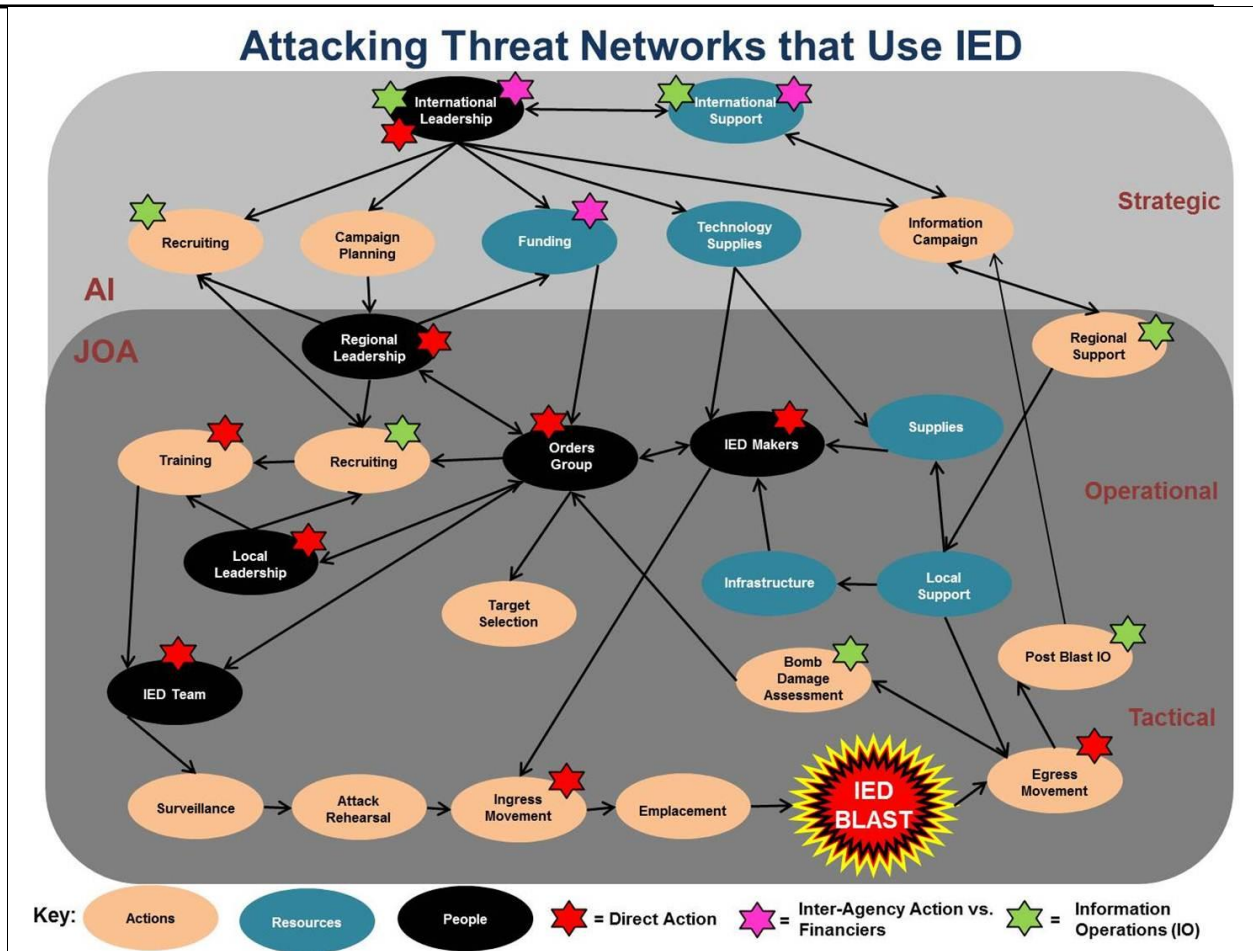


Figure 14 - Multi-Level Attack Against an IED Network

8. At the operational level, commanders focus on the threat networks that are active in their assigned operational area. Through the use of specialized analytical tools, commanders will be able to refine their understanding of the OE and focus resources on key nodes in the network's infrastructure. For example, geospatial intelligence can be used to identify threat network nodes such as safe houses, bomb construction locations and cache sites. Operational level organizations normally develop detailed plans for attacking critical network nodes and coordinate with tactical units for actual execution. Operational commanders will usually supplement the tactical echelons with specialized AtN/CTN enablers (intelligence collection and analysis, forensics, special operations, and others) to facilitate their operations. When operating in sectors, units employ their intelligence capabilities and employ specialized network enablers to develop an extended intelligence picture and response options. They coordinate and inform lower echelons of the effects desired, ensure unified actions are taken to favourably shape the OE, and employ IO to influence the friendly, neutral, and threat network actors and nodes. The focus at the tactical level is on executing AtN/CTN and providing accurate feedback to the JIPOE process. Accurate, timely and relevant intelligence will drive this

effort. Tactical units exercise refined procedures to conduct analysis, create a template and then target networks. In a COIN operation, for example, friendly tasks include efforts to secure the population, strengthen HN security forces, and counter the enemy's ideology and propaganda. See "AJP 3.4.4 Counterinsurgency." These efforts contribute to the overall AtN/CTN effort by serving to isolate the threat network from its supporters, suppliers and sympathizers. Tactical units will also conduct precise exploitation, kill, or capture operations, often founded on dynamic targeting. In Figure 15 below are examples of some of the types of AtN/CTN related activities that can be conducted by a Joint Force at the tactical and operational level in the conduct of AtN/CTN operations. In addition, for Allied and Partner nations, strategic options are also provided:

ACTIVITIES	TACTICAL ACTIONS	OPERATIONAL FUNCTIONS	STRATEGIC OPTIONS
Understanding the Networks	JIPOE (AO & AI), Key Leader Engagement KLE), Network Nodal Analysis, Human Terrain Teams (HTTs) -- Cultural specialists, Advanced Situational Awareness Capability (ASAC)/Combat Hunter, Advanced Situational Awareness Policing (ASAP)/Combat Policing	JIPOE (AOR), ISTAR	Strategic Intel, Foreign Service engagement (UN, Law Enforcement, Commerce, Embassy, etc.)
Network Exploitation	Biometrics, Technical Intelligence, DOCEX, Computer Network Operations (CNO)	MASINT, ISTAR	MASINT, HUMINT
Search	Overt and/or Discreet	Resource and train	MASINT
Lethal and Other Kinetic Operations (Kill/Capture)	Small Kill Teams (SKTs), Combat Patrol, Detention Operations, High Value Targeting Teams (HVTs)	HVI, HVTs, Time Sensitive Targeting (TST), Interdiction Operations	HVI (Top Tier), Covert and Clandestine Operations, Law Enforcement Apprehension
Non-Lethal/Non-Kinetic Influence Operations	Information Operations, CIMIC, Psychological Operations, Public Affairs	Information Operations, Public Affairs, Security Cooperation	Public Diplomacy, Démarche, Economic Sanctions or Benefits
Networks Infrastructure Interdiction	CNO, Counter Threat Finance (CTF), Cordon & Search, Checkpoints	CTF, CNO, Import Controls	CNO, CTF, Sanctions
Reinforcing Friendly Networks	Info & Intel sharing, Mobile Training Teams (MTTs), Joint Combined Exchange Training (JCETs), Enhanced Military Education and Training (E-METs),	Security Cooperation Activities	Foreign Support funding & authorities including Military Assistance (Foreign Military Sales, Foreign Military Financing, Transfer of Excess Defense Articles), International Law Enforcement training
Populace & Resource Control (PRC)	Covert Surveillance, Neighborhood Watch, Population, Vehicle, & Firearms Registration/mapping, Checkpoints & Inspections	Import Controls, Border Security, Biometrics database, Law Enforcement Interface	Sanctions, Import and Immigration Controls

Figure 15 - Possible AtN/CTN Activities at the Tactical and Operational Levels

Targeting the Network

9. Friendly, neutral, and threat networks must be methodically targeted to achieve the desired effects consistent with the commander's intent and the joint operation/campaign objectives. The Joint Force and staffs need to establish an integrated process to identify targets, determine the desired effects on those targets, predict second and third order effects, and execute non-lethal and lethal operations to achieve those effects, see figure 16 below.

10. The Joint Force establishes priorities and synchronizes the efforts of subordinate organizations through an iterative planning process. Within the framework of the joint operation/campaign plan, the Joint Force components and units use a targeting process which applies multiple assets, on multiple levels, to develop and prosecute targets. The joint targeting cycle provides the mechanism which translates the commander's guidance and targeting objectives into actions to engage targets through both lethal and non-lethal means. A comprehensive targeting program requires participation from the entire staff and specialized enablers from external civil organizations and military forces. At a minimum, an operations/intelligence, time sensitive targeting cell, will be established to develop actionable intelligence to target threats in real-time and a longer term planning cell will address continuous development of AtN/CTN targets.

11. In real terms, targeting of threat network critical vulnerabilities is driven by the situation, the accuracy of intelligence, and the ability of the joint force to quickly execute various targeting options to achieve the desired lethal and non-lethal effects. In AtN/CTN activities, threat actors and nodes that perform tasks that are vulnerable to detection/exploitation and impact more than one critical requirement are a higher priority for targeting. However, while a paymaster is a critical target the day before payday, that actor is less valuable a week after payday as you move up the financial chain seeking the funding source before the next payday. Timing is everything when attacking a network and in an irregular warfare environment, the opportunities for attacking identified critical vulnerabilities are limited.

Target Types.

12. There are basically two types of AtN/CTN targets; those that must be dealt with immediately (such as HVI) and those longer term network infrastructure targets (caches, supply routes, safe houses) that are normally left in place for a period of time to allow for longer and deeper exploitation of them. Additionally, when defining target priorities, consideration should not be limited to only HVIs. Operations in Iraq and Afghanistan have demonstrated the effectiveness in targeting the middle-layers of networks nodes and actors and servicing them near simultaneously, thereby degrading a large "chunk" of a network. Resources to service/exploit these targets are allocated in accordance

with the Joint Force's priorities, which are constantly reviewed and updated through the command's targeting coordination mechanisms. This allocation is validated through a daily asset synchronization meeting and breaks down into two main types of targeting:

- a. *Dynamic Targeting.* A time-sensitive targeting cell consisting of operations and intelligence personnel, with direct access to lethal means and the authority to act on pre-approved targets, is an essential part of any AtN/CTN effort. Using a dynamic targeting process, the cell services targets that have been identified too late or not selected in time to be included in deliberate targeting or that meet High Value criteria specific to achieving the stated objectives.
- b. *Deliberate Targeting.* Organizing the participants in the targeting process can be accomplished through the standard boards, working groups, and cells process. One approach is to establish a Joint Fires Cell (often called a "fusion centre") to provide mission analysis planning, execution oversight, coordination, and critical liaison duties that reach from the strategic and operational levels to the tactical level. A Joint Fires Cell is given responsibility for refining targeting in coordination with the intelligence cell, and coordinating the daily management of the close air support allocation and apportionment for the command's area of operation. The cell also provides field grade and company grade officers to multinational, interagency (as required), and HN partners. These officers perform duties ranging from fire support officers, information operations experts, to targeting officers. The Joint Fires Cell is tasked to look at an extended timeline for threats and the overall working of threat networks. With this type of deliberate investigation into threat networks the cell can identify catalysts to the threat network's operations and sustainment that had not traditionally been targeted on a large scale. With a constant flow of intelligence about individual actions and movements, the cell will examine what facilitated any number of events, such as terrorist, criminal or narcotics activities, failed public services and governmental corruption. It will also focus on how these events ultimately impact not only the Joint Force's operations in support of the overall joint operation/campaign plan, but also international development and aid efforts together with the local government and population. This type of analysis will usually reveal a web of interconnected relationships and associations of which only a small percentage can be affected by lethal targeting and actions. When augmented with appropriate non-military, special operations, and HN intelligence analysts, the Joint Fires Cell can plan to exploit these relationships and associations using non-lethal means and seek to reduce their contribution to the overall effectiveness of the enemy's network. At the Joint Force, the Joint Fires Cell (or its equivalent) develops AtN/CTN related targets to nominate to the joint targeting

coordination board for approval and subsequent execution on an on-call or deliberate basis.

Targeting Methodologies.

13. The joint targeting cycle provides a framework to describe the steps that must be satisfied to successfully target threat network nodes or links. Currently, there are three primary targeting methodologies within phase five (mission planning and execution) of the joint targeting cycle. Depending on the situation, multiple methodologies may be required to create the desired effect. The three primary methodologies are:

- a. *D3A*. This is “*decide, detect, deliver, assess*”. It is a deliberate and dynamic targeting method.
- b. *F2T2EA*. This is “*find, fix, track, target, engage, assess*”. This is essentially a dynamic targeting methodology.
- c. *F3EAD*. This is “*find, fix, finish, exploit, analyse, disseminate*”. This is a dynamic targeting methodology

14. All of these methodologies, including F2T2EA, supports the joint targeting cycle execution phase and facilitate the servicing of time sensitive targets (TST). The F3EAD model was developed for personality-based targeting and has been widely adopted as the principal targeting process for AtN/CTN. Successful employment of the D3A and F3EAD methodologies requires the assignment of persistent surveillance assets.

Operations / Intelligence Cycle

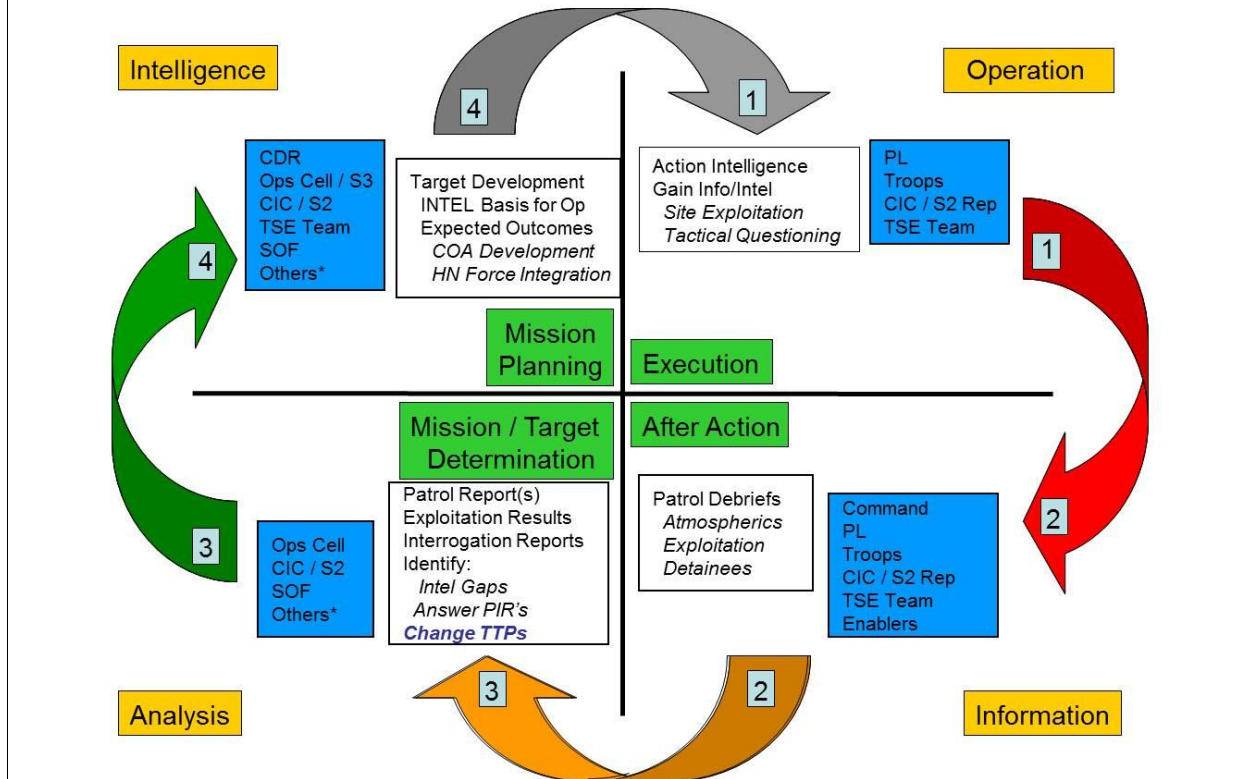


Figure 16 – Ops/Intel Cycle

Fixing and Finishing Options

15. There are a number of options:

a. *Strengthening and Protecting Alliance Networks.* Seeing where the network exists and operates outside the theatre of operations must be the focus at the strategic level. Separating the threat network from external sources of finance, recruiting and material resources is the most important strategic level action to strengthen and protect the Alliance objectives and friendly networks. This often means comprehensive approach engagement with third parties at a strategic level and involves national level intelligence, law enforcement, and diplomatic agencies taking the lead in achieving strategic aims. There are some operational functions which help to protect Alliance objectives and friendly networks:

(1) *Operational Functions.* Operational functions to strengthen and protect Alliance Networks often focus on the training and equipping of tactical formations, but also include the development of goals and outcomes to gain unity of effort among all the agencies and actors operating in theatre. Important aspects are:

(a) *Information Exchange.* (see Chapter II)

(b) *Enabling and Protecting Partner Networks.* There are two complimentary methods:

i. *Capacity Building.* Capacity building can be defined as providing infrastructure to the partner network or host nation. It involves activities along all lines of operations but is usually focused on security, economic and political capacity. Once the mechanisms and institutions are built, the responsibility to execute and sustain capacity must be transferred to the partner network/nation.

ii. *Capability Development.* While the coalition may have to do these functions initially, the long term objective is to build the capacity for minimum acceptable capability performance by the partner (network or nation). This is the essence of T.E. Lawrence's 15th Article.⁷

b. *Interdicting and Neutralizing Adaptive Threat Networks.* When conducting AtN/CTN operations to interdict and neutralize the Threat Networks, it is important to keep the following general framework in mind:

(1) Begin with understanding the desired outcome or effect. The specific outcome or effect of Joint Force operations must be the first factor known and considered. This understanding comes from well-articulated commander's intent and from detailed mission analysis.

(2) Determine your timeline for achieving that specific outcome. If the Joint Force has a lot of time to accomplish the specific outcome, the

⁷ *Do not try to do too much with your own hands. Better the Arabs (insert: Host Nation) do it tolerably than that you do it perfectly. It is their war, and you are to help them, not to win it for them."*

- T.E. Lawrence, *Twenty Seven Articles*, Article 15

steps and risks taken are different than when the outcome or effect is needed immediately. This is especially true when working to influence neutral networks in conjunction with interdicting the threat networks.

- (3) Understand tasking and resourcing processes and timelines to reinforce friendly networks. AtN/CTN activities against threat networks often require a mix of organic and higher headquarters resources. Proper synchronization of those resources requires an understanding of the time requirements and processes needed to bring those assets and their effects to bear on the threat network.
- (4) Understand the nature of the threat network in time and space. Because the JTF is working toward a specific outcome, understanding how the Network exists and operates is critical to achieving an overall effect. That said, accomplishing an outcome in one area, may have adverse effects on friendly operations and outcomes in another area where the threat network exists and operates. Subordinate organization activities must therefore be coordinated and synchronized by higher headquarters to achieve harmonized outcomes across the entire OE.
- (5) Understand the friction between collection and targeting. The intelligence and operations communities might have differing opinions as to the opportunity of engaging a threat network. Deciding when to act on or against a node or actor of the network who is unwittingly providing intelligence on his or the network's activities, capabilities and intentions, can be difficult. Only the commander can make this decision but it must be informed by good staff analysis of the benefits and risks of continued collection versus immediate action.

c. *AtN/CTN Operational Functions and Activities.* First and foremost, efforts at the operational level must focus on synchronizing tactical actions and prioritizing and allocating resources to reinforce friendly networks. The distributed nature of networks means that tactical formations will rarely have operational control of all the terrain where the network exists and/or operates. Actions by one tactical formation against one part of the threat networks can have serious negative effect on the efforts of other tactical formations and other parts of the Alliance networks. It is incumbent on the operational level Joint Force HQ to coordinate and synchronize the intelligence collection and operational actions of subordinate formations. Additionally, the operational level HQ must prioritize and manage the allocation of limited assets, in theatre, so they may be used to best effect—i.e.

best effects in strengthening Alliance networks, influencing neutral and attacking threat networks within the overall campaign objectives.

d. *AtN/CTN Tactical Activities and Tasks.* While AtN/CTN tactical activities are determined largely by unit capability and mission, some fundamentals remain the same. First in order of importance is the need to fuse operations and intelligence into a unified cycle and not allowing these activities to operate in isolation of each other. Second, formations must resource and empower tactical units at the lowest level possible; if companies are operating out of a remote combat outpost, they must have the ability to conduct intelligence/operations fusion at their level. This stems from the requirement to see and understand the network locally as well as getting the overall assessment from higher headquarters. Third, tactical units must engage, develop and partner with other elements of the Alliance and neutral networks in their AO. Unity of effort and gaining the trust and confidence of these other elements are necessary conditions to successfully attacking the threat network to achieve Alliance objectives.

e. *Integrating AtN/CTN Enablers.* The exact actions to integrate enablers will depend on the capabilities and limitations of those organic and attached enablers. There is a fundamental truth that enablers must be integrated as early as possible in the planning process and this must be continued throughout the analysis and exploitation of their efforts. Enablers generally fall into the following categories:

- (1) ISTAR (Collection)
- (2) Analysis and Exploitation
- (3) Influence Operations
- (4) Capacity Building (CIMIC)
- (5) Capability Building (Training)
- (6) Kill/Capture specialist capabilities (SOF and specialized conventional forces)

16. AtN/CTN, as any type of operational activity, is designed to leverage traditional military tactics and operational functions, but also, importantly, it requires a broad comprehensive approach as well as the ingenuity of the friendly network. Maintaining a flexible approach to conducting operational and intelligence fusion is necessary.

Ensuring effective Intelligence lead operations is critical to AtN/CTN success. The Joint Force Commander and Staff need to make sure well targeted and flexible methods, procedures and actions are employed in order to properly engage Networks in the OE.

Assessment

17. Commanders and staffs at all echelons need to be able to measure the effectiveness of their operations in order to refine subsequent operations. Measures of Effectiveness (MOEs) and Measures of Performance (MOPs) need to be determined and the necessary resources allocated to collect data against indicators of effectiveness.

18. Since human based networks are inherently open systems, predictability of effects are difficult to determine. Consequently, assessment relies on continuously monitoring and evaluating the current situation and the progress of an operation. In AtN/CTN, commanders and staffs must constantly assess the impacts that their operations have on the targeted networks (Blue, Green, White, Black and Red) and the population that is the focus of network influence. They must look “multiple moves ahead” to consider the second and third order, and any potential cascading effects their actions may have on their envisioned outcomes and how those actions will impact both the threat and friendly networks as well as the population.

19. Continuous comprehensive holistic assessment is critical to the success of an operation. Apparent initial success can lead to disastrous consequences without a well-organized assessment plan. The threat network adapts and these adaptations must be taken into account when executing the AtN/CTN plan.

Conclusion

1. While this handbook provides recommendations to implement AtN/CTN in Alliance operations, it is in no way prescriptive. However, in addition to the overall framework recommended, critical elements of AtN/CTN include the recognition that the Alliance operates in a dynamic OE permeated by networks that do not necessarily operate according to the time-honoured rules of nation state interaction.
2. AtN/CTN requires effective intelligence lead operations that require a new degree of command decentralization and subordinate initiative. It also demands an engagement process that incorporates the comprehensive approach that goes beyond the traditional military solutions and emphasizes information sharing.
3. Moreover, AtN/CTN is only effective in organizations that can function with maximum flexibility, creativity and agility. As previously stated, in order to defeat threat networks, it takes other networks that can operate within the threat networks decision-cycle (Observe-Orient-Decide-Act).