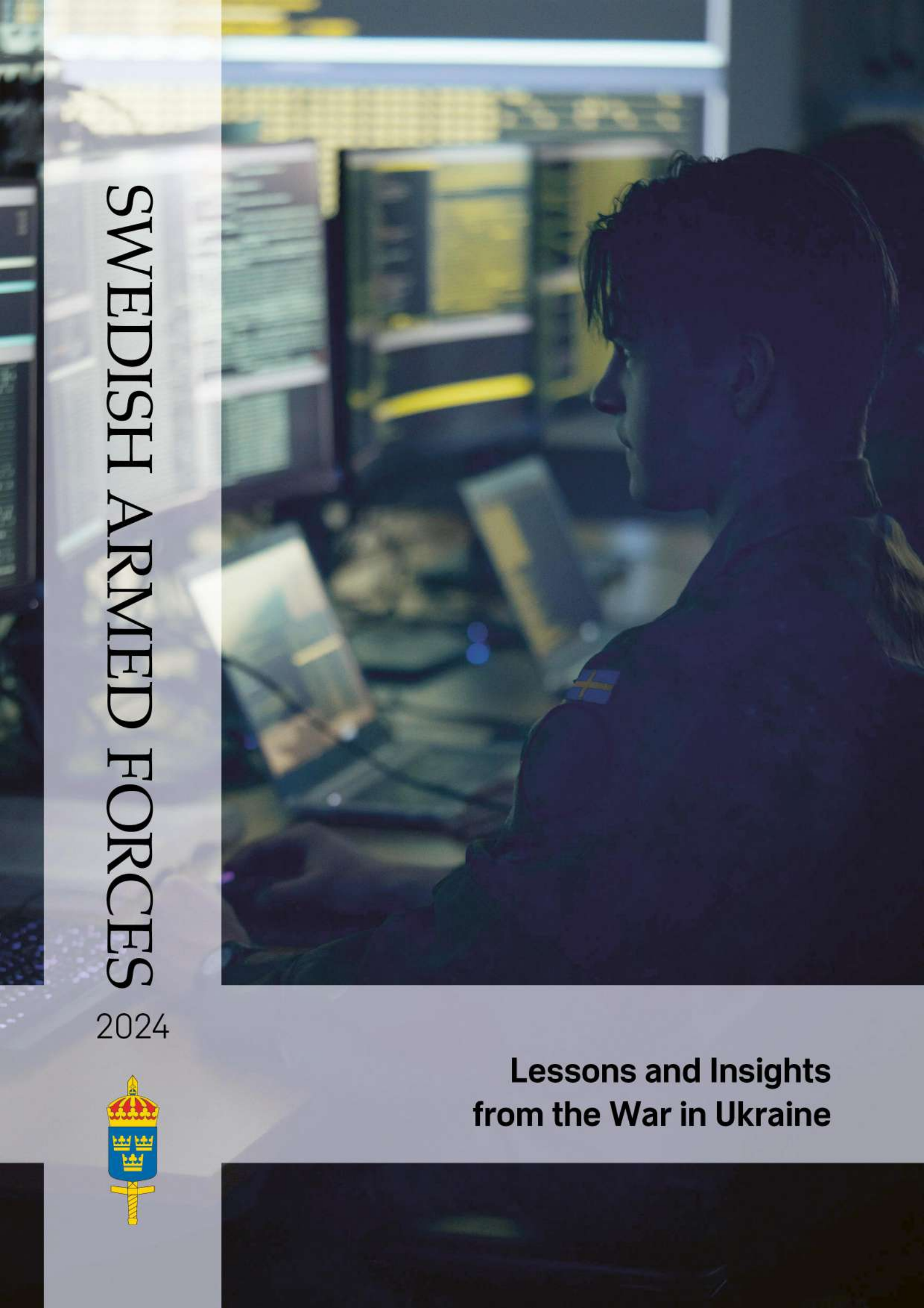

SWEDISH ARMED FORCES

2024

Lessons and Insights from the War in Ukraine

Swedish Armed Forces Lessons and Insights from the war in Ukraine

In July 2023, the Government commissioned the Swedish Armed Forces to report on how lessons and insights based on the war in Ukraine can be implemented in the Swedish Armed Forces' operations and in the continued development of military defence.[1] On November 2, 2023, the Swedish Armed Forces submitted an initial report to the government.[2] This report is the Swedish Armed Forces' final report in completion of the government assignment.

This report further analyses the lessons from the war in Ukraine presented in the Armed Forces' initial report of November 2, 2023. The lessons described are captured as inputs in the continued development of the Swedish Armed Forces, for example in doctrine development, planning, exercises, training and education. However, the Swedish Armed Forces emphasises the importance of rigorous practices for implementing lessons learned. A number of processes are therefore being developed to increase the effect of the Swedish Armed Forces' lessons learned efforts.

The Swedish Armed Forces will continue to analyse lessons from the war in Ukraine and refine the process for doing so. New methods and forums for inter-agency collaboration have also been established in conjunction with the development of the Swedish Armed Forces' lessons learned processes. The Swedish Armed Forces will continue to deepen these collaborations in order to strengthen its organisational learning capability and thereby enhance the Swedish Armed Forces' abilities and operational effects.

[1]Government decision, Fö2023/01323, 2023-07-13
[2]The Swedish Armed Forces' Lessons from the War in Ukraine, FM2023-2379:9

(MAU)

Mailing Address	Visiting Address	Telephone	Fax	E-mail, Internet
Försvarsmakten	Lidingövägen 24	+46 8 788 75 00	+46 8 788 77 78	exp-hkv@mil.se
SE-107 85 Stockholm				www.forsvarsmakten.se
SWEDEN				

Method

This report does not suggest how the lessons should be addressed, given the ever-present risk that observed phenomena and experiences from the war are unique in time and space and thus not relevant for future warfare. However, the report emphasises the importance of incorporating insights and lessons as it is likely that the phenomena described will be integral components of future conflict scenarios.

The dynamics of war suggests that a particular lesson that is domain-specific at one point in time may become applicable to another domain at a later point in time. The pace of technological development and adaptation of tactics during the war carries the risk of drawing conclusions based on individual experiences. The war in Ukraine needs to be analysed in the broader context of other wars and conflicts as well as technological leaps.

This report is not intended to be a comprehensive account of lessons from the ongoing war in Ukraine, but to present and analyse a selection of observed phenomena. The selection is primarily based on analysis and discussions conducted both within and between academia and various militaries that are deemed influential for the future development of warfare.

The Swedish Armed Forces has continuously monitored the war in Ukraine and sought to gather information and lessons from the war from a variety of sources. These sources include partner countries, Ukrainian representatives, the defence industry and relevant authorities, particularly with support from the Swedish Defence Research Agency and the Swedish Defence University. This support has been in the form of seminars, workshops, meetings and interviews. Specialists in various fields have also contributed with their expertise.

Reading guide

Chapter 1 describes relevant Ukrainian lessons in more detail based on what was described in the Swedish Armed Forces' initial report to the Swedish government on November 2, 2023.

Chapter 2 describes and analyses the significance of these lessons.

Chapter 3 describes and summarises how Sweden's and NATO's warfare could develop in the coming years.

Table of Contents

Introduction

Putin's War?

> *[...] Crimea, the ancient Korsun or Chersonesus, and Sevastopol have invaluable civilizational and even sacred importance for Russia, like the Temple Mount in Jerusalem for the followers of Islam and Judaism.*[3]

There is reason to consider the ongoing war in Ukraine as part of a more extensive great power competition. In this great power competition, Russian rhetoric about the war is based on a number of assumptions about Russia's historical role. The Russian approach to an existential war in Ukraine as thus goes well beyond the period of President Vladimir Putin. The Western notion of the war as 'Putin's war' can therefore be seen in a broader context.

Russia's annexation of the Crimean Peninsula in 2014 can be seen in the historical context as a military strategic choice to maintain Russia's access to an ice-free port in the Black Sea, which Russia has sought since the time of Catherine the Great and the creation of the Black Sea Fleet. The Christianisation of the Kievan Kingdom in the 10th century depicts the beginning of the Russian creation myth, i.e. the story of how Russia and its worldview were formed. This was the reasoning Putin chose to present to the Russian people in his 2014 address to the nation to explain and justify the annexation of Crimea. In Putin's own words it was also not possible to allow 'NATO boots' on land that is sacred to Russia.

Sevastopol, on the Crimean peninsula, has been the base of the Russian Black Sea Fleet for over 200 years and is one of twelve Soviet hero cities. Sevastopol is therefore central to the mythology of Russian military power. Russia has, lost the city at times during a number of wars leading to national wounds. After the dissolution of the Soviet Union, Russia and Ukraine have negotiated on several occasions to continue to allow Russia to use the city's naval base.

The war in Ukraine is part of a Russian rationale of an existential war associated with the creation myth in the form of the narrative of a patriotic defensive war and in which the West acts as the aggressor. Today, Putin uses the idea of a patriotic war in order to strengthen national cohesion and justify Russia's warfare. Regardless of assumptions about whether the war will continue after Putin or not, the Russian Armed Forces will continue to evolve and adapt, both doctrinally and in terms of capabilities.

---

[3]Putin, Vladimir. 2014. *Presidential Address to the Federal Assembly.* http://en.kremlin.ru/events/president/news/47173

The Dynamics of War

The war is characterised by two post-Soviet military systems facing each other. Both adversaries use new equipment and technology and develop tactics and combat techniques, mainly to survive on the battlefield and limit the opponent's ability to act. Ukraine has received support and advice from several Western countries. This means that Ukraine is developing a hybrid of Soviet thinking, Western influences and new thinking based on its own experiences. However, no new operational concepts or principles have yet been observed.

Almost no major joint operations have been conducted, and have sometimes been fully or partially abandoned in favour of unilateral ambitions in a specific domain. This has demonstrated the importance of creating dilemmas for the adversary in all domains and at all levels of warfare in order to force the adversary to prioritise and thereby retain the initiative. The war has also led to attrition as well as wear and tear of both Russia's and Ukraine's traditional military platforms. Tanks and armoured vehicles are more often destroyed by hard to detect unmanned platforms that are small, fast, cheap and easy to develop. Ukraine has also sunk a third of the Russian Black Sea Fleet, not through major naval battles, but through the use of unmanned vehicles and land based systems.

The initial Russian invasion in 2022 was a failure, and the subsequent period of fighting in Donbas region was initially characterised by Russian fire superiority. In addition to precision munitions, the use of unmanned aerial vehicles for target detection improved the effectiveness of the older Russian artillery systems. Russian artillery batteries using unmanned aerial vehicles for target detection also proved capable of firing on Ukrainian positions within minutes of detection. This forced Ukrainian infantry to spread out in order to survive. Consequently, battalions covered front widths which traditionally would be the responsibility of a brigade. Russian artillery superiority and sensor density also prevented the Ukrainians from concentrating in units above company size since larger unit formations would be detected early and could be combatted effectively at long distances.

Both Russia and Ukraine have had integrated air defence systems sufficient to successfully deny the other party from establishing sufficient control over the air. This means that neither side has had sufficient capability to achieve air supremacy. However, Ukraine has maintained central command of its air defence forces. This has had a positive impact on the ability of its forces to defend against a much larger opponent. Ukraine has also demonstrated the ability to detect and counter Russian long-range weapons, such as cruise and ballistic robots.

The lesson is that battlefield conditions can make it difficult to concentrate forces to carry out offensive operations. This reduces the likelihood of large-scale combat and requires a synchronisation of effects, rather than a traditional concentration of forces. This in turn places an additional burden on command and control capabilities, especially when it is jammed by electronic warfare.

Moreover both Russia and Ukraine strive for superiority in their respective kill chains while at the same time prioritising to disrupt each other's kill chains.

Russian Capability for Military Adaptation

The ongoing war in Ukraine has acted as a catalyst for tactical and military-technological adaptation. Both Russia and Ukraine have adjusted and adapted their societies to the demands of war. Both countries are adapting based on lessons learned and their experiences from the war.

The Russian Armed Forces are characterised by top-down management, a legacy of the Soviet era that initially made military adaptation difficult. The same top-down approach is now being used by the military leadership to remove barriers to adaptation and systematise change across the Russian defence sector. What still hampers Russian adaptability is the fear of reprisals for reporting failures in the Russian Armed Forces.

Russia's adaptability has improved since its full-scale attack on Ukraine. Two contributing factors are the transition to a war economy and cooperation with countries such as China, Iran and North Korea. This has enabled increased production of military equipment, including ammunition and drones. The increased production has in turn resulted in greater freedom of action to introduce military adaptations. To summarise, Russia is perceived as a change oriented adversary whose toolbox has few limitations in pursuing its long-term strategic objectives. Still, Russia's tactics is largely based on a war of attrition where the Russian approach and higher level innovation process, has been characterised by 'more of everything'.

1. Battlefield Transparency and the Future Operating Environment

> *You go to war with the army you have, not the army you might want or wish to have at a later time.*[4]

This chapter describes a number of observations from the war in Ukraine that demonstrate an evolution of warfare. Most notable is the phenomenon that, after the Ukrainian offensive in the spring of 2023, the war has transitioned to trench warfare, with Russia and Ukraine each struggling to break through the defensive lines of the other. This is partly due to extensive field engineering protected by mines and artillery. Efforts to break through lines of defence are further complicated by the density of sensors, which create a combat environment that has been named 'the transparent battlefield'.

The lines of defence, especially those of Russia, are comprised of extensive fortifications such as trenches, barbed wire and tank obstacles protected by mines and artillery. The Russian ability to re-mine cleared segments using remote mine delivery systems is a challenge for Ukrainian counterattacks. This has allowed Russian units to maintain control over large areas of land.

On the transparent battlefield, the operational environment is flooded with different sensors – mainly unmanned aerial vehicles – and all troop movement and military activity is closely monitored, especially in the land domain. The transparency of the battlefield in the maritime domain is less obvious, though its implications are often more far-reaching and sometimes global. As a result of battlefield transparency in Ukraine, dispersion has proven a determinant of survivability to such an extent that force concentration has been made difficult. The war is now fought mainly by small units that have been difficult to coordinate to achieve operational effect, when attacking as well as holding captured terrain.

Another feature of the transparent battlefield is increased precision for long-range fires, as a result of which both parties have withdrawn command and logistics resources as far as possible from the front line. While both sides continue to adapt, neither has recently achieved decisive operational or strategic success due to difficulties in force concentration. The ground war should also be considered in the context of the lack of air supremacy and the imbalance within and between the domains.

The transparent battlefield, especially by means of unmanned aerial vehicles, has accelerated the cat-and-mouse game between who is the best at hiding and the best at striking first. The large number of sensors combined with tactical

---

[4]Rumsfeld, Donald. 2004. *Troops Question Secretary of Defense Donald Rumsfeld about Armor.* https://www.pbs.org/newshour/show/troops-question-secretary-of-defense-donald-rumsfeld-about-armor

adaptations based on lessons learned has led both sides to continually raise the tempo of their kill chains. In previous wars and conflicts, Western countries' drones for reconnaissance, localisation, target tracking and assessment have been an exclusive and costly resource. The war in Ukraine shows that relatively inexpensive drones can be used for these purposes in most domains, including jamming global navigation satellite systems (GNSS).

1.1. Unmanned Vehicles

The field of unmanned vehicles, also referred to as drones, has presented the greatest breadth of both needs and solutions; it is characterised by constant change and adaptation. What is new is that drones are now increasingly deployed in the sea and land domains. The use of drones in the air domain has also evolved, with more uses, new countermeasures and new drone types – most notably first person view drones.[5] To cover huge losses, in some cases estimated at 10,000 per month, large numbers of commercial aerial systems are being procured and adapted in Ukraine and near the battlefield. The development of unmanned systems shows that they have been used both as a force multiplier and as a function or service branch by itself. In February 2024, for example, Ukraine established a new service branch for unmanned systems.

During the war in Ukraine the use of unmanned systems has been the main reason that it is next to impossible to hide in the battlefield. This applies mainly to the land domain, but developments in the sea domain are increasingly innovative. In addition almost all physically visible infrastructure is mapped by various sensors. Unmanned vehicles have the advantage that a single platform can be used for reconnaissance, surveillance and combat at a relatively low cost. The low cost also means that the battlefield can be flooded with drones to saturate any defences. Suicide drones, known also as kamikaze drones, have been described as the most effective type of unmanned weapon system, posing a greater threat than conventional artillery, with the potential change in tactics due to a lack of artillery force concentrations.

Drones are increasingly used as decoys to induce the opponent to activate its air defence sensors, which can then be targeted. This approach further exemplifies that precision strikes, by means of an effective kill chain that continually adapts to changing conditions, are more effective than a wide-ranging artillery fire, from which both sides have learned to protect themselves.

The challenge with remotely operated and autonomous systems is that many such systems depend on electromagnetic communication that is vulnerable to electronic warfare.[6] Remotely operated and autonomous systems in the maritime

[5]A drone with a camera that directly transmits what it sees to the operator, usually via a pair of glasses.
[6]Within 12 months of the widespread use of suicide drones with control links on the 900 MHz bands, Russia had fielded countermeasures.

domain are less dependent on GNSS and less reliant on electromagnetic signals than airborne systems. This includes torpedoes, mines and various remotely controlled unmanned craft.

In the air domain, there are efforts to make systems less vulnerable to jamming by making them more autonomous and less dependent on positional information from global navigation systems. Communication links are also modified to use different frequencies in an attempt to avoid jamming, which in turn requires rapid adaptation of countermeasure systems. Furthermore, systems are now commonly deployed in tandem, with larger craft in the rear serving as communication relays while smaller systems that are more difficult to detect operate over enemy-controlled territory.

The lesson for the Swedish Armed Forces is to increase access to different types of unmanned vehicles in order to learn how to use them effectively, and how best to defend against drones in different conditions. Conditions need to be conducive to train with and against drones at all levels. This needs to be done broadly within the Swedish Armed Forces as different units have different needs and conditions. The different types of restricted sites also present different attributes and preconditions that factor into how they can best be protected.

The challenge in developing effective countermeasure systems against drones (Counter Unmanned Aerial Systems, C-UAS) is the wide variety of drones they face. Success requires multiple modes of protection, for example movement, speed, jamming, camouflage, decoys, close air support and nets, as currently there is no single comprehensive system. This problem has led to a reappraisal of the importance of physical protection and combat engineering at the tactical level as well as for operational logistics and command and control. In order to clarify all these needs and limitations, this topic should be further investigated with the support of other government agencies, but coordinated by the Swedish Armed Forces on the basis of a common goal for total defence.

1.2. Electronic Warfare

The war in Ukraine has highlighted the need to be able to operate and understand one's own footprint in the electromagnetic spectrum and ranging from positioning systems, coordinating the safe timing of communication and not least for controlling remotely operated vehicles or using autonomous systems. Extensive electronic warfare operations, both jamming and scanning, underline the need to master one's footprint in the ether and determine prudent transmission practices. A wrong decision leads to attracting incoming fire, often within a short time. Both Russia and Ukraine have used the entire electromagnetic spectrum to communicate during the war, and there are hardly any frequency bands dedicated for civilian use that remain. Instead, transmission capabilities have been multiplied by using both commercial and military communication systems.

The struggle between measures and countermeasures stimulates technological development in electronic warfare, which is so rapid that new technologies quickly becomes obsolete. A common example is jamming satellite systems from drone-based or ground-based jammers. These jamming systems range from large ground-based high-power systems to micro-systems with low power, which are nonetheless sufficient to prevent, e.g. space-based sensors from identifying vehicle types. As a result there is a need for highly automated electronic warfare capability that quickly adapts to changes in the adversary's technical systems. This technology has been relatively expensive and exclusive, but this field is developing at a fast pace. Heavy and high-power jamming systems targeting a wide frequency carry the risk of interfering with one's own systems and revealing the position of the jammer. The most attractive option is to use many small, light and mobile systems, however this may trade off against automation, since smaller and light systems usually lack this capability. Whatever the solution may be, an effective electronic warfare capability must be combined with frequency planning and coordination.

Despite electronic warfare capabilities and signals intelligence, both sides in the war continue to use the mobile phone network and the internet, albeit in different ways. The use of mobile phones and military radio systems at the front line continue to pose a high risk of exposing units of enemy fire. Incoming fires may follow within minutes of starting a mobile phone call. Therefore, applications such as *Discord*, *Telegram, Signal* and *WhatsApp* are widely more used than mobile calls and military radio systems, as a combination of different internet solutions is perceived as the most secure with the commercial satellite system *Starlink* being used frequently. However, what Ukrainians emphasise is the importance of disseminating information quickly and widely. These applications also facilitate transmission of images and videos, which enables the sharing of data collected by drone operators.

Using commercial applications or broadband infrastructure carries risks, such as interception or tapping. For Ukraine, the advantages have so far outweighed the disadvantages, and the potential Russian capabilities for signals intelligence, or acquisition in the cyber domain, have not had a significant effect. Regardless, this is an example of how different domains and functions interact with and within each other, demonstrating that the Swedish Armed Forces need to have the capability to track and influence both military and commercial systems at the same time. A delegated mandate for electronic warfare has proven to be crucial in both offensive and defensive operations.

1.3. The Cyber Domain

Cyberattacks have been a recurring feature, targeting various sectors of an increasingly digitalised Ukraine. Since the start of the war in 2014, Ukraine has had to create an organisational structure, at the central and local levels, capable of managing cyber threats and keep military and commercial IT systems operational.

Coordinating the country's cyber security resources, including volunteers, has been a key experience in balancing the requirements of information confidentiality, accuracy and availability with an operational perspective. The experiences from the war in Ukraine shows the importance of having cyber expertise and incident management capabilities, both in local organisations and centrally to create a robust organisation.

Almost all analogue communications systems are being phased out as systems are increasingly connected to digital networks. As a result, implementing cyber defence capabilities is even more critical. This also applies to military systems, e.g. space-based assets, electronic warfare assets and other sensors as well as artificial intelligence (AI) need to be integrated via command and control (C2) systems for operational impact. Overall, the digitalisation of society where physical systems are highly integrated tends to lead to the importance of electronic warfare, signals intelligence, C2 systems as well as intelligence collection in the cyber domain.

Ukraine has demonstrated how the cyber domain can be practically integrated into joint operations by using cyber assets to find suitable targets. This can be achieved either by exploiting IT vulnerabilities of a previously identified high-value target or by scanning for sensors that the adversary has connected via the internet (e.g. remote-controlled cameras). In addition, developments in artificial intelligence have opened up new possibilities in the cyber domain, especially for intelligence purposes for analysis of images and video, and even at the tactical level, e.g. by enabling real time monitoring of troop movements.

The continuous proliferation of software in military systems entails a growing need to continuously protect systems, data and information and to update software while making information available. The war in Ukraine also shows that the digitalisation of society creates a need for a coherent cyber defence capability with aligned structures at all levels of command that also has the ability to collect intelligence in the cyber domain which can contribute to joint fires and effects.

1.4. The Space Domain

A number of upheavals are underway in the space domain. On the one hand, countries are undergoing a paradigm shift and view space as a military operational domain and are adapting military structures and capabilities accordingly, and on the other hand, commercial space systems play an increasingly important role in modern warfare. The latter has shed light on the ambiguity of whether commercial space systems should be considered civilian or military for the purposes of military attacks, an issue with no international consensus as yet. For Ukraine, the use of commercial space systems has increased its defence capability since these could not be unequivocally classified as military targets by Russia, although during the war Russia has stated that commercial satellites that contribute to the war could be classified as legitimate military targets.

Today, Russia's position as the third space superpower is diminished, and is clearly lagging behind the United States and China in terms of both technology and numbers. Nevertheless, Russia's ability to use space systems for military purposes should not be underestimated. Although Russia faces considerable and multifaceted challenges in the space domain, the country has a wide range of space-based and space-denying capabilities aimed at inhibiting the use of their space-based systems by other actors.

In the war in Ukraine, space-based systems have been used as a force multiplier by both Russia and Ukraine. For example, the combination of space systems with unmanned vehicles and long-range weaponry has been shown to enhance the ability for deep strikes. The idea is certainly not new, but as the technology within these systems becomes more accessible, these resources can be used at all levels of command providing an enhanced capability to both strike deep and protect tactical assets.

In Ukraine, commercial space systems have been used in warfare at an unprecedented scale. Commercial systems are often comprised of larger constellations of up to several hundred satellites, which individually may be low performing but collectively enable completely different services than those of military systems, which are traditionally based on larger single satellites with high performance. This, combined with the continuing development of the space domain, including offensive space capabilities, raises questions such as whether procuring few and expensive satellites creates a major vulnerability in the system. Cheaper and thus more satellites create redundancy and secure access to space services, even if one or more satellites were to be disrupted or otherwise affected. It also makes it possible to separate civilian and military use of satellites to a greater degree.

Commercial earth observation satellites enabled the public to follow the Russian troop build-up in the media through daily images even before the start of the invasion. In addition, intelligence and analysis could be shared more easily between countries as it was based on public images without revealing their own military intelligence collection capabilities. Ukraine has procured large amounts of commercial earth observation data, but also purchased an ICEYE SAR radar satellite through crowdfunding. There are reports that in the first two days alone, this satellite detected 60 Russian units, resulting in Russian loss of materiel far more than the total cost of the satellite. This demonstrates the value of satellites as a force multiplier for other military systems.

The war in Ukraine has shown that satellite systems can be of great importance to both the military and civilian society. This has highlighted the importance of safeguarding space infrastructure and its capabilities from disruption or attack during a conflict. *Starlink,* which provided Ukraine with communications and internet, has had to actively update its cyber security during the war to ward off attacks aimed at affecting the system. It is also obvious that the clear strength of

Starlink lies in the number of satellites it consists of, as well as the speed and ability of *SpaceX* to launch new satellites. The lesson for Sweden is that countries that want satellite systems for different purposes, must see that the security, protection and defence of their own space capabilities is of paramount importance.

1.5. Command Post Survivability

The transparent battlefield combined with more and cheaper weapon systems with longer ranges creates significant threats to command posts, both fixed and mobile. This is in addition to a trend whereby Western military staffs have grown and command posts have come to include more technology. Larger command posts generate more movement and also emit a larger electromagnetic footprint, making such command posts easier for an adversary to detect via drones, signals intelligence, cyber domain intelligence and satellite systems.

The fact that command posts, especially in Western countries, have increased in size is a consequence of the increase in the complexity of the battlefield, partly due to hybrid threats and partly due to technological developments driving cross-domain impact and integration. The debate on command post survivability has revolved around traditional issues of self-protection such as camouflage, deception and physical protection, including anti-aircraft and C-UAS.

More difficult issues in the area of command and control (C2) are how to reduce command posts, how command resources can be dispersed more widely, how camouflage can be improved, and how the logistical and electromagnetic footprint can be reduced. Masking is significantly easier and cheaper in terms of optical camouflage while acoustic, thermal and electromagnetic camouflage is more expensive. Reducing the logistical footprint is possible, for example, by enforcing strict routines for inflows and outflows from command posts, with some goods and services possibly being delivered via unmanned vehicles.

The greatest challenge is to reduce the electromagnetic footprint, especially as dispersion leads to increased transmission and thus emission. In this area, a number of solutions have emerged from the military debate. One solution is to deploy command posts, to the extent permissible by international law, among existing infrastructure so that emissions do not stand out to any great extent. Another solution is to make greater use of commercial communications systems in order to conceal military transmissions. Another example is to use communication technology with a narrow and targeted emission, such as laser. In all likelihood, no single solution is sufficient; instead, a combination of measures will be required to conceal one's own command and control resources as much as possible.

1.6. Operating in the Information Environment

Since the full-scale invasion in 2022, Ukraine has had two main objectives for strategic communication. Firstly, to maintain the population's will to defend itself and secondly, to secure the support of the Western world. A few overarching narratives have been used to adapt the focus and form of the communication to reach different target groups. To secure the West's continued support in the war, Ukraine has, among other things, launched social media campaigns aimed at the populations of countries that have donated weapons systems. In the campaigns, Ukraine expresses gratitude to the countries' populations, often with a humorous touch.

Ukraine has created a broad situational awareness of its relationship with Russia. Creativity and the pursuit of information superiority have contributed to success in the information environment in collaboration with intelligence services and international actors. Additional success factors cited by the Ukrainian Armed Forces include coordinating available resources and cooperating with external actors. This has been a prerequisite for maintaining a rapid pace, adding new ideas as they come and publishing communications in several languages.

The media has an important role in how the image of the war is conveyed and thus perceived by various actors. At the outbreak of war, martial law was declared and shortly afterwards an order was issued by the Commander-in-Chief for military censorship. This has had a major impact on the media's ability to report on the war. In a protracted war, balancing the state's interests with journalistic integrity and media independence can prove challenging. In this regard, Ukrainian conditions differ from those of Sweden, but the question of the role of public service in the event of war is complex, partly because there is a challenge in finding a balance between the need for operational security and transparency in communication.

To make an impact in the information environment and win the battle for the narrative, it is important that the entire organisation strives towards the same strategic communication objectives and goals. These objectives and goals should be clear but general. Mission command is necessary to act quickly in the information environment and to win the battle for the narrative. In addition, there is a need for a robust and well-distributed battlefield documentation capability in the event of war, since the ability to quickly use relevant imagery in communications is a success factor.

Society's ability to communicate and achieve information superiority is contingent on a resilient information and communications infrastructure. At the start of the full-scale invasion, Russia attacked Ukraine's ground-based communications infrastructure while satellite company *Viasat* was subjected to a cyber-attack. The solution to this was the widespread introduction of *Starlink* in Ukraine. *Starlink* has also enabled information to flow both in and out of Ukraine. This has helped the civilian population to keep abreast of events, but also to share information about life in war-torn Ukraine and the need for international support.

Situational awareness, information superiority, ownership of the narrative and the ability to orchestrate and manoeuvre, i.e. continuously adapt communication to achieve the desired military strategic effects, needs to be an ongoing process. The lesson for the Swedish Armed Forces and total defence is that resources for planning, implementing and analysing effects and communicative outcomes for one's own part and for the adversary, needs to be in place early and this creates the preconditions for joint operations.

1.7. Conclusion – The Importance of Surprise, Deception and Camouflage

The transparent battlefield has forced a reappraisal of surprise, deception, concealment, camouflage and decoys. This applies to all military activities and in all domains. In addition, civilian resources such as ambulances and rescue vehicles have also had to be camouflaged to avoid fire. The transparent battlefield, combined with the lack of air supremacy, has contributed to an inability to concentrate force in space. Moreover, limitations in the ability to concentrate forces, command larger units and conduct joint operations were visible before the war transitioned to trench warfare.

The transparent battlefield has also demonstrated the difficulty of achieving surprise and deception on a local and tactical level. The lesson is that the latter requires planning and coordination at the strategic and operational levels in order to achieve operational effect. Political actions ultimately determine the war outcomes, but such action is usually taken in the wake of pivotal operational success. Operational success is in turn made possible by adaptability with innovative solutions at the tactical, operational and strategic levels. The war in Ukraine shows, for example, that false signalling and information operations take place at all levels of command.

The Swedish Armed Forces needs to develop a refined capability to hide on the transparent battlefield and simultaneously saturate the opponent's systems. This requires the Swedish Armed Forces to test, exercise and challenge the organisation. This encompasses the use of surprise, deception, concealment, camouflage and decoys as well as measures to reduce electronic emissions. This requires the Swedish Armed Forces to train and utilise *Red Teams*[7] authorised to reconnoitre acoustically, optically, thermally and electromagnetically to build an understanding of how the Swedish Armed Forces appears in the eyes of the adversary. For this reason, legislation and regulations need to be to be updated on an ongoing basis, especially regarding the regulation and coordination of low-altitude airspace. Regulations need to accommodate rapid coordination and review of regulations regarding intelligence collection, reconnaissance, surface surveillance, protection and combat.

[7]Red Team testing is used either to evaluate one's own organisation by simulating a threat actor's attack methods or to generate alternative action options.

2. The Tempo of Warfare

Operational tempo is a state of mind.[8]

There is an ongoing debate within both academia and the military profession about how the development of warfare in Ukraine will affect military operations, theory and doctrine – now and in the future. The reason is that the war in Ukraine has led to an increased focus on the need for flexibility and military adaptability, especially as technological developments have opened up new opportunities and at the same time created new challenges. This chapter describes these opportunities and challenges.

According to the fundamentals of tactics, sufficiently favourable conditions need to be created in relation to the opponent in question, which is usually called local superiority. Local superiority can be created through force concentration, surprise and freedom of action. In Ukraine, the transparent battlefield has significantly impeded both surprise and force concentration, which in turn has led to limited freedom of action in achieving the desired effect. In order to succeed, force concentration must be sufficiently covert or rapid that the opponent is unable to respond adequately. A high operational tempo in turn requires the ability to lead and coordinate the battle as well as access to intelligence.

Technological developments and the transparent battlefield demonstrate the importance of having faster decision loops than the opponent. As described, the integration between domains, sometimes also in combination with artificial intelligence, means that much of command and coordination happens in real time. This places great demands on mobility in general, but foremost on the need for decision-making dominance over the opponent. Decision-making dominance refers to the ability to integrate and coordinate all domains to achieve an effective kill chain.

The command and control requirements of high tempo warfare place increased demands on intelligence services to detect, assess and deliver target data for high-value targets. In addition, methods and resources are required to evaluate whether combat is generating the intended effect, and if not, to propose new objectives. It has been a topic of discussion to what extent achieving these things will require an increased use of autonomous systems, to include systems powered by artificial intelligence.

2.1. Dispersion and Forward-deployed Command Posts

Striving for and achieving smaller staffs and command posts can be advantageous for mobility, logistics and footprint, which in turn means an increased ability to operate covertly. Smaller staff size also facilitates protection of the staff site including concealment and camouflage. However, utilising fewer personnel

[8] Mattis, Jim & Bing, West. 2019:103. *Call Sign Chaos: Learning to Lead.* Random House.

presents the challenge of physical endurance and sourcing the breadth of skills required across functions and domains, especially at higher levels of command. At lower levels of command, the help of user-friendly C2 systems for decision-making could be important, but does not negate the need for a wide range of competence within the staff. However, this requires that all levels of management have the ability to contribute with necessary and scalable information to the situational picture.

One way to adapt the size of staffs is to make them scalable and modular. This would lead to increased flexibility based on the prevailing situation and conflict intensity, which is of importance in order to quickly increase or strengthen C2 capabilities in time and space. This is of particular importance with Sweden's NATO membership, partly because different countries contribute with different C2 capabilities that Sweden needs to cooperate with, and partly because the Swedish Armed Forces' extended area of operations entails command from greater distances. The greater distances and higher pace place new and increased demands on C2 capabilities and endurance.

The increased demands on C2 capability can be mitigated to some extent by dividing staffs into a number of smaller units interconnected in a network of several forward, middle and rear command locations. These can in turn be supported by a prepared number of fixed or mobile command nodes. Pre prepared nodes and scalable, modular staffs provide command resources to 'leapfrog', both in time and space, which in turn reduces the risk of lapses in decision-making. An extended 'C2 network' also means that rear command posts act as support (Reach-Back), and can be gradually reinforced over time as needed. This places new demands on technical solutions such as modern and relevant staff and command posts.

2.2. The Need for Tactical ISR Capabilities

The transparent battlefield places increased demands on the amount of intelligence, surveillance and reconnaissance resources (ISR), especially at the tactical level of command where the pace of decision-making is highest. This is salient in the context of the war in Ukraine with its large number of unmanned aerial vehicles for reconnaissance and surveillance. Smaller commercial drones are limited by their short ranges and susceptibility to jamming, although technological development show that the range is gradually being extended. In other words, other types of reconnaissance capabilities are also required, above all in the field of electronic warfare. Reconnaissance in the space and cyber domain can often take place at higher levels of command and as Reach-Back, but needs to be processed and coordinated at the tactical level. The disadvantage of these disciplines is that they are technology-heavy and require expertise, while electronic warfare capabilities are developing at an ever increasing pace.

If anything, the war in Ukraine has shown, that there is no single superior intelligence collection discipline, but that the combination of disciplines and the ability to adapt collection to prevailing constraints and needs is the key to

success. For example, the acoustic and thermal information collection is increasingly emerging as a success factor, in part because it can be done from any platform, including drones, and because sensor technology is more resistant to electronic warfare. Although Ukraine is continuously updating its C2 systems, there are challenges in coordinating and integrating information from different intelligence collection disciplines.

With today's technological development, the Swedish Armed Forces have an increased possibility to test and learn more about using tactical ISR resources on a large scale as both the quality and cost of unmanned vehicles, acoustic sensors and commercial satellite services are falling. In addition, Sweden can utilise its domestic development and production capacity. The pace of technological development means that it is not possible to wait for a complete solution; instead, the learning and introduction of different sensors and how they can best be used must take place incrementally.

2.3. The Kill Web

Having a faster kill chain than the opponent means the opportunity to strike first at high-value targets. A degradation of the opponent's component capabilities hopefully diminishes their overall C2 capability. In other words, there is danger in focusing on individual (high-performance) systems instead of command and control coordination, which is crucial for optimising combat in time and space, and is also time and resource-intensive to build up once wiped out.

The war in Ukraine has shown that both Russia and Ukraine have different strengths and weaknesses in the kill chains. Ukraine's main strength lies in prioritising command and control capability, by continuously developing the C2 system *Delta* and prioritising speed and information sharing (the push principle) over information security. As Ukrainian supplies of ammunition have dwindled, the need to locate high-value targets on a minute-by-minute basis has grown. This has proven to be a challenge for both sides, as they have learned to continuously regroup units exposed to enemy fire.

A further challenge of the transparent battlefield is that large amounts of information need to be processed and made comprehensible in order to make informed decisions quickly. This is an aspect of decision-making dominance, knowing which resources can achieve the best results where, when and possibly how. As technology developments increasingly enable information and intelligence from multiple domains, decisions in multiple kill chains become increasingly complex. This complexity points to a need to move away from kill chains to kill webs since intelligence, combat information and weapons systems interact and support each other in both time and space.

For the success of kill webs, artificial intelligence has been described as a crucial future component. Nonetheless, one must not forget that any effective kill web relies on competent staff and an organisation with creative and decisive decision

makers. Regardless of how artificial intelligence continues to develop, it is highly likely that defending against a skilled adversary with AI-enabled decision-making will be problematic if one's own organisation does not use artificial intelligence. The degree of automation that is appropriate in decision-making will however be a subject of debate for many years to come. Regardless of the degree of automation, technological developments show an increased need for C2 systems with integrated decision support with simple and clear options for decision makers, including options when sensors or combat systems fail for some reason.

2.4. Situational Awareness and Visualisation

The complexity that follows from greater access to information across domains and levels of command brings opportunities as well as new challenges in presenting information that is comprehensible. The war in Ukraine shows that even if C2 systems can present geographic information with the option of overlaying intelligence or information about their own operations, some information is best presented two-dimensionally while other information is best presented three-dimensionally. A further question is whether certain information is best presented graphically, symbolically or as an image, or alternatively as a combination of all.

At the combat and tactical levels, there is technology that can improve both image quality and simplify how images are presented from different sensors in real time. The technology also offers the possibility of superimposing information from different sensors so that it is easy to zoom in and out of the area of operations. This means that previous limitations of UAS and satellite based sensors due to weather conditions in the Nordic region are now virtually eliminated. However, assimilating information remains labour intensive, even if artificial intelligence is introduced to control unmanned vehicles and how their video feeds are presented.

The challenge of creating a common operational picture based on information from all domains is knowing what type of information should be presented at what time and to which decision makers. What artificial intelligence can offer in this regard is decision-making tools that can learn to link information needs to different types of operations, to different functions and to different decision makers, where it is also quick and easy to choose from different presentation options. In this field there is much to learn from the computer game industry. The challenge for the Swedish Armed Forces is finding a balance between robust military C2 systems that are also interoperable, and existing civilian technologies and skills similar to how Ukraine developed the *Kropyva* application or the *Delta* C2 system. Furthermore, clear chains of command are needed that allow mechanisms to disseminate information about the situational picture in the cyber and space domains at the tactical, operational and strategic levels of command.

2.5. The Use of Civilian Communication Technology

Since 2014, Ukraine has progressed technologically with the support of a number of leading global providers of services and equipment in the telecom and IT sectors. There are lessons to be learn there about the value of state-business relations and the role business can play in total defence. One conclusion is that a variety of different suppliers creates technical diversity in C2 systems. This means that different suppliers do different things or, for that matter do similar things but in different ways. This may have its disadvantages from an end-user perspective but it helps avoid monocultures within IT.

From a purely military perspective, the war has been characterised by how civilian technology is used, not least in the form of so-called 'dual-use' products, where technical solutions can be applied for both civilian and military purposes. The use of commercial technology in a military context has resulted in good technological dissemination, not least through the use of the space domain, which in itself has created resilience and an opportunity to defend and keep systems operational.

The advantage of also being able to use commercial communication systems, the mobile phone network in combination with existing broadband infrastructure, is that it creates redundancy as these systems are inherently relatively resistant to jamming. Fibre-based systems also have the added benefit of not having the emission that link-based communication systems have. 4G and 5G mobile networks can furthermore be used for encrypted communication without using mobile phone calls, which is particularly important for the quick and easy transfer of images and videos. Mobile networks also facilitates the wide sharing of information, which is of particular importance during higher levels of conflict and mobilisation.

The lesson for the Swedish Armed Forces is to find a balance between information access and information security, especially if the trend is towards greater use of commercial communications technologies, including 4G, 5G and satellite communications. In addition, the war has raised the issue of secure procurement where unsecure commercial solutions can lead to undesirable effects. One such example is the leakage of geographic data. The lessons also show the importance of utilising civilian resources to maintain a high tempo without compromising cyber security.

Another lesson for the Swedish Armed Forces is to strike a balance between military C2 systems and commercial communication systems to maximise redundancy. This also applies to storage services and whether these should be cloud-based or not. Military cloud-based solutions are under development and the Swedish Armed Forces needs to explore these possibilities.

The Ukrainian C2 system *Delta* is particularly highlighted as an interesting example because the system has a cloud solution with servers located abroad, making it impossible to physically attack the system in Ukraine. The C2 system works more like a social media platform than a traditional system. Connections can be from a

plethora of platforms and authentication relies largely on the phone or the computer's own system with the user configuring their role in the system. Principles of trust come into play when systems are designed this way and the loss of hardware connected to the system is a problem that needs to be addressed.

2.6. Conclusion – Fail Fast, Fail Early!

The combination of deteriorating geopolitical conditions and rapid technological development places distinctive demands on the Swedish Armed Forces to simultaneously grow, develop and integrate into NATO. What the war in Ukraine has shown, apart from the fact that development is fast, is that working solutions must be rapidly procured and produced in sufficient quantities. There also needs to be a large and flexible training organisation so that solutions can be implemented to full effect. Unfortunately, rigorous procurement of new materiel systems and the development of new capabilities are very time-consuming processes. As previously described, long development cycles pose a significant risk in the context of the geopolitical developments and rapid technological advances. Capabilities and technologies can quickly become obsolete and the Swedish Armed Forces risks missing opportunities to learn new capabilities. This risk is not unique to the Swedish Armed Forces: many countries face the same difficult choices.

The solution being discussed in NATO to deal with the above risks is for armed forces to rapidly experiment with new things and learn from mistakes, thereby reducing the consequences of incorrect decisions. At the moment, neither Sweden nor NATO is engaged in high-intensity conflict and therefore there is an opportunity to fail and learn in a safe environment alongside allies and partner nations. But to succeed in this, the Swedish Armed Forces needs to adopt a new approach to risk-taking, including the approach to C2 systems and information security. Instead of risk aversion, concepts such as innovation, creativity and lessons learned analysis need to take centre stage. Military units, schools and centres need to participate actively in experimentation and trial and error activities where the interfaces with the private sector are more interactive and parallel than sequential.

The lesson for the Swedish Armed Forces is that the organisation needs to be adaptable, with the mandate and capacity to continually develop technical solutions with a decision-making cycle that is quicker than that of the adversary. In addition to a developed lessons learned process in the Swedish Armed Forces there is a need for industry, academia and other defence authorities to be a natural part of the Swedish Armed Forces' schools and centres in a triple helix model. This can hopefully lead to a blurring of the boundaries between training, development, lessons learned process and innovation where different competencies support as well as challenge each other. The Swedish culture and spirit of entrepreneurship should be particularly conducive to such a solution, which in turn will hopefully foster the ability to carry out multi-domain operations.

3. The Operational Art of the Future

> *The basic cognitive skill for dealing with surprise is creative thinking since only this type of mental activity can improvise effective solutions.*[9]

As described in the previous two chapters, there are a number of contradictory trends in the evolution of warfare. These challenges need to be solved not only by the Swedish Armed Forces, but also by our allies in NATO since nations have different strengths and weaknesses that need to be managed in order to create a common deterrent. Integration and adaptability enable the Swedish Armed Forces to conduct operational art together with our allies based on a desired outcome.

3.1. The Need for Simplicity in an Increasingly Complex World

In order for the Swedish Armed Forces to conduct operations at a higher pace than the adversary, decision-makers need to practice and be trained to coordinate military activities with non-military activities in all domains, environments, and at all levels of command. Today's technological developments makes it possible to conduct multi-domain operations to a higher extent than before. Thus, advanced technical systems, primarily in the cyber and space domains and in the information domain, need to be made available faster and on a wider scale within total defence.

The development of advanced technical systems demonstrates the possibility of analysing, presenting and visualising a shared situational picture that incorporates information from all domains. Technological development also enables simplified and flexible tools to achieve rapid decision-making. The Swedish Armed Forces therefore needs to move towards a more software- and application-centric technology instead of platform- and network-based system solutions. In the long term, development will probably also need to move towards completely data-centric solutions that are fully independent of both applications and platforms.

3.2. Operational and Decentralised Decision-making

Operational art generally is not technology-driven, but the conduct of operational art is always technology dependent. For example, knowledge of the operational environment, including the adversary and other actors, is a necessity for conducting operations. Today's modern technology expands the opportunity to present and visualise selected information at all levels of command. In other words, advanced technology provides commanders at all levels with new opportunities to gain awareness, insight, and understanding of the operational picture – and of how their functions and responsibilities fit in – which is an enabling factor for joint operations. This lays the foundation for mission command and mission discipline with the ability to quickly take responsibility

[9] Finkel, Meir. 2011:100. *On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield.* Stanford Security Studies.

and initiative. To take advantage of this opportunity, decisive and creative commanders should have permissive mandates with clear strategic and operational objectives. This development also needs to be reflected in both doctrine and organisation.

The war in Ukraine has shown the importance combining capabilities to achieve effects at the tactical, operational and strategic levels, which can cause strategic dilemmas with limited resources. The increased access to information provides opportunities to exploit weaknesses of the adversary in all domains and at all levels of command. For example, targeting strategic objectives such as key infrastructure has previously required deliberate and carefully planned efforts with strategic resources. Now, resourceful and creative lower-level commanders with offensive cyber capabilities or access to drone technology can also conduct these types of operations. The conclusion is that these opportunities and challenges need to be addressed doctrinally by a well-trained and competent organisation able to use doctrines without compromising innovation and adaptability. To succeed in this, the Swedish Armed Forces needs a broader training portfolio and the option to recruit personnel with new skills.

3.3. Multi-domain Operations – A Journey into the Future

The war in Ukraine has demonstrated how cyber and space capabilities complement and enhance capabilities in the three physical domains of land, sea and air. This has happened spontaneously rather than being the deliberate product of a joint operational capability. The conclusion is that advanced technology does not necessarily have the desired operational outcomes unless organisation and doctrine are also developed in a coherent system of systems approach. Therefore, NATO is now developing the concept of multi-domain operations (MDO) where the main idea is to orchestrate all military activities, in all domains, with non-military activities (*synchronise*). This increases the possibility of creating desired effects in the virtual, cognitive and physical dimensions at the speed of relevance.

The future operational environment and the operational concepts formalised in multi-domain operations may be perceived as technology-driven, but primarily constitute a cultural shift in the conduct of warfare. This places new demands not only on our soldiers, sailors and officers, but also on everyone who operates within the framework of total defence. Organisation, management processes, training and leadership must therefore be adapted to meet these demands.

Sweden's NATO membership entails that we do not have to face these challenges alone. Instead, it is important to allow incremental development, i.e.to start with the most important functions and thereafter make successive additions and changes. By continuously supporting development with evaluation and lessons learned analysis, Sweden's military capabilities and that of the alliance can form a credible and coherent whole that can handle future challenges.

The Swedish Armed Forces wrote this report in collaboration with the Swedish Defence Materiel Administration, the Swedish Civil Contingencies Agency, the Swedish Defence Research Agency and the Swedish Defence University.

- o0o -

This report has been authorised by Lieutenant General Carl-Johan Edström.

Carl-Johan Edström

Chief Joint Operations

Distribution list
SWE MILREP NATO
Releasable to NATO