April **2023**

Freedom of Manoeuvre in Cyberspace

Joint Air Power Competence Centre

Cover picture: Ⓜ © Valery Brozhinsky/Shutterstock.com

A special thanks to the following people for providing clarification and recommendations during the drafting of this document:
Lieutenant-Colonel (FRA) Jeremy Merlin, European Air Group
Lieutenant-colonel (EST) Urmet Tomp, NATO Cooperative Cyber Defence Centre of Excellence
Major (LTU) Gediminas Venckus, NATO Cooperative Cyber Defence Centre of Excellence
Commandant (IRL) Rónán Micheal O'Flaherty, NATO Cooperative Cyber Defence Centre of Excellence

Authors
Lieutenant-Colonel Eric Jodoin (RCAF)
Major (ret.) Fotios Kanellos (HAF)

Disclaimer
This paper is a product of the JAPCC. It does not represent the opinions or policies of the North Atlantic Treaty Organization (NATO) and is designed to provide an independent overview, analysis and food for thought regarding possible ways ahead on this subject.

Terms of Use – Alteration, Notices
This White Paper may be reproduced for instruction, reference or analysis under the following conditions:
1. You may not use this work for any commercial purposes, nor may it be used as supporting content for any commercial product or service.
2. You may not alter, transform, or build upon this work.
3. All copies of this work must display the original copyright notice and website address.
4. A complete reference citing the original work must include the organization, author's name, and publication title.
5. Any online reproduction must also provide a link to the JAPCC website www.japcc.org, and the JAPCC requests a courtesy line.
6. This White Paper made use of other parties' intellectual property in compliance with their terms of use, taking reasonable care to include originator source and copyright information. The originator's terms of use guide the reuse of such material. To obtain permission to reproduce such material, please contact the copyright owner of such material rather than the JAPCC. In case of doubt, please contact us.

Release
This document is approved for public release. This document is distributed to NATO Commands. Nations. Ministries of Defence and relevant Organizations. Portions of the document may be quoted without permission, provided a standard source credit line, 'Courtesy of JAPCC' is included.

Published and distributed by
The Joint Air Power Competence Centre
von-Seydlitz-Kaserne
Römerstraße 140
47546 Kalkar
Germany

Telephone: +49 (0) 2824 90 2201
Facsimile: +49 (0) 2824 90 2208
E-Mail: contact@japcc.org
Website: www.japcc.org

Follow us on Social Media

Ⓜ Denotes images digitally manipulated

FROM:
The Assistant Director of the Joint Air Power Competence Centre (JAPCC)

SUBJECT:
Freedom of Manoeuvre in Cyberspace

DISTRIBUTION:
All NATO Commands, Nations, Ministries of Defence and Relevant Organizations

The decades bracketing the year of the 'Y2K bug' heralded a transformation in the world where the increasing use of computing technologies worked to improve the lives of just about every human being in unprecedented ways. The 'Y2K bug' itself taught us that this emerging domain, which we would later call cyberspace, remained rather immature. The mostly peaceful use of the nascent cyberspace domain has been increasingly contested over the last two decades by various agents: Criminals, hacktivists, disgruntled employees, and state actors have all been bent on exploiting flaws in the still nascent cyberspace domain to achieve nefarious goals at the expense of individuals, whole nations, and everything in between.

Military organizations worldwide have benefited from the growth in computing technologies and the emergence of cyberspace to improve their Observe/Orient/Decide/Act (OODA) loops with the objective of gaining information superiority and, by extension, an edge on the battlefield. But, as we increasingly rely on computing technologies and cyberspace, we also seek 'efficiencies' to help control the rising costs of maintaining and operating a modern, computerized, and interconnected warfighting force. This has had the unfortunate consequence of introducing vulnerabilities and single points of failure, which are now threatened by an explosion of actors in cyberspace with varying degrees of competence and capabilities.

Cyberspace permeates all other warfighting domains. In a Multi-Domain Operations (MDO) framework, it is the glue that joins and enables seamless, synchronized operations. Therefore, as leaders within our own warfighting domain, we must demand, expect, and invest our scarce resources to help grow cyberspace capabilities that are vital to our national and combined operations. This white paper is intended to help raise the level of understanding required to do just that.

Paul Herber
Air Commodore, NE AF
Assistant Director, JAPCC

JOINT AIR POWER COMPETENCE CENTRE
Joint Air Power Competence Centre | von-Seydlitz-Kaserne | Römerstraße 140 | 47546 Kalkar | Germany
Phone: +49 (0) 2824 90 2201 | E-Mail: contact@japcc.org | www.japcc.org

This Page Intentionally Left Blank.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

NATO defines manoeuvre as 'Employment of forces on the battlefield through movement in combination with fire, or fire potential, to achieve a position of advantage in respect to the enemy to accomplish the mission'. But how does this definition apply to a nascent cyberspace domain? The objective of this paper is to help warfighters better understand cyberspace operations and explore what might constitute Freedom of Manoeuvre (FoM) in cyberspace. NATO has no doctrinal definitions for FoM in cyberspace. Therefore, this paper proposes that manoeuvre in cyberspace can be interpreted as the methods and processes employed to attack and defend systems and information resources to give one actor a competitive advantage over another.

To achieve its objective, this paper introduces the reader to cybersecurity and cyber defence fundamentals. To prevail in cyberspace, three components must be preserved: The confidentiality of the data, the integrity of data and systems, and the availability of data and systems. This is commonly referred to as the CIA Triad. In order to preserve the CIA triad, we must maintain cyberspace Situational Awareness (SA) to understand the space we operate in, including the infrastructure and the data within it. Next, we must develop adequate risk management models to identify and mitigate threats and vulnerabilities. Finally, we need a defensive cyberspace operation mechanism capable of dealing with breaches whenever the mitigation measures are overcome.

Cyberspace permeates our everyday lives. It was introduced to automate and expedite repetitive tasks and help humans deal with increasingly complicated problems. OODA loops are particularly well suited to allow automation of repetitive tasks that do not require human judgment; whomever can iterate through their descision processes the fastest gains a decisive advantage on any competitive endeavour, including warfare. Therefore, the system of systems that are OODA loops were early adopters of cyberspace technologies and continue to push the boundaries of the possible by adopting Emerging and Disruptive Technologies (EDTs) to automate tasks once considered unsuitable for computers. Adoption of computers and EDTs brings a suite of challenges including the risks of failing to fully secure and defend them, in accordance with the cybersecurity fundamentals discussed earlier. Russian's quick deployment of a new cryptophone shortly prior to the start of the Ukrainian invasion and it's almost instantaneous failure at the war's onset is such an example. While EDTs should not be considered a cure-all, it does provide us with new opportunities and threats. Therefore, chapter 5 is dedicated to EDTs and will cover the impact on FoM in cyberspace brought about by EDTs such as 5G, Artificial Intelligence (AI), and Quantum Computing (QC).

With a basic appreciation of cybersecurity fundamentals and how OODA loops are enhanced through the effective use of cyberspace, it becomes possible to tease out the unique characteristics of cyberspace. Speed and operational reach can very quickly deliver effects against a great number of geographically separated targets. Rapid concentration and distribution becomes possible through automation to overwhelm a single target through fires coming in from innumerable points of origins across the world. Dynamic evolution plays a disproportionate role in evolving and transforming cyberspace at a rate never experienced by mankind before. Finally stealth and associated difficulties in attribution significantly complicates established international laws and norms regarding the proportionality and scope of a response.

Another key element to any manoeuvre is the identification of terrain, particularly key terrain. Because of the unique characteristics of cyberspace listed previously, it is often hard to identify relevant key terrain at any one time. However, there is one constant that transcends all recorded failures to defend in cyberspace: All attackers managed to circumvent or

overcome authorization and authentication measures, making these the highest of high grounds regardless of the circumstances. It is also the reason why the cybersecurity industry as a whole is moving toward a 'zero trust' model where authorization and authentication takes centre stage.

The zero trust model is especially applicable to NATO as the organization is taking a data-centric approach to multi-domain operations where data sharing, data exchange, data appreciation, and data exploitation become the nexus to enable fully synchronized cross-domain and cross-nation military operations in the ultimate instantiation of the OODA loop. This vision for MDO will only be achievable if FoM in cyberspace can be preserved while being denied to our adversaries.

Finally, as we increasingly rely on technologies to enhance military capabilities, soldiers will be increasingly reliant on equipment and weapons platforms that depend on cyberspace to fulfil its function. Therefore, they will no longer simply be frontline fighters in their respective domain (air, land, sea, space); these conventional physical assets simultaneously occupy the frontline of cyberspace and their operators may be the first to observe attacks directed at them (or their equipment) through cyberspace. Therefore, military personnel of all branches will need to be adequately trained to deal with threats and attacks emanating from cyberspace and strongly supported by organic cyberspace capabilities such as incident response and hunt teams intended to blunt any such attacks. The concept of cyber FoM provides the lexicon and framework to make this vision a reality.

CHAPTER 1

Introduction

1.1 Cyberspace Origins

When the term cyberspace (from cybernetics and space) was first introduced in 1982 by the author William Gibson, his intention was not just to describe the Internet itself, together with its required network topologies and Information Technology Infrastructure (computers, servers, routers, controllers, and other components).[1] His aim was to depict an emerging, amorphous, and virtual place consisting of a plethora of links acting as intermediary nodes in a global digital network. Cyberspace would become the place created by these links; a unique space for developing human interactions and communities where information, ideas, and values would travel across the world rapidly.[2]

Later, during the 1990s, John Perry Barlow[3] would use the word cyberspace to refer to 'the present-day nexus of computer and telecommunications networks.'[4] Today, with the advent of sophisticated robots, advanced automation, and the development of new and emerging technologies such as Artificial Intelligence (AI) and quantum computing, the meaning of cyberspace has significantly expanded to include activities and tasks performed even without human intervention.

The prefix cyber derives from the English noun cybernetics, taken from the Greek word kybernetes (κυβερνήτης). The latter means helmsman or governor and implies how essential it is in a purely virtual environment to control the speed and maintain the initiative of movements and operations among various (virtual) spaces.

In modern times, cyberspace is considered a highly contested and challenged domain, characterized by conflict and rivalry among states, non-state actors, criminals and insiders; navigating in safe 'territories' and under controlled conditions is vital for mission assurance in cyberspace. Since 2017, NATO has already recognized that '…most crises and conflicts today have a cyber dimension…'[5]

Recognizing that anyone relying on and using cyberspace in the conduct of their activities finds themselves on the frontlines of cyberspace. This paper aims to provide the required knowledge and explore the main elements of what constitutes FoM in the cyberspace domain and how this can be ensured in a continuously evolving multi-domain security environment.

1.2 Background

The principle of manoeuvre has always had a significant value in military thinking and warfare operations since the early ages. In almost all decisive battles in history, both sides would attempt to defeat the opponent by incapacitating his decision-making and disorganizing him through shock and disruption. To achieve this goal and bring about a positive outcome, it was crucially important to determine which positions the conflicting forces would move before and during combat in relation to their opponent.[6]

One of the most famous manoeuvre acts on the battlefield was during the Battle of Marathon in 490 BC, where the Athenian and Platean Forces joined to counter the Persian attack. Miltiades, the Athenian general, not only chose the field tailored to his needs, with marshes and mountainous terrain that would prevent the Persian cavalry from joining the infantry, he also reinforced his flanks, lured the Persians into the centre, and systematically enveloped and defeated them. This underlines a simple truth: Effective manoeuvre can create success on the battlefield.

In the later centuries, the military theory of manoeuvre would be successfully adopted and practised during the expansion of warfare into new domains. The development of naval forces, aviation capabilities, and space assets provided new environments in which military forces engage in or enable warfare.[7] The exploitation of the seas, the air, and outer space have evolved into new battlefields and frontiers in modern military operations where each domain developed its own doctrine of manoeuvre.

Despite (or perhaps because of) the tremendous technological evolutions and unique scientific developments that are widely available today, the necessary level of FoM in the military cyber domain has not yet been achieved. Both in the physical and virtual worlds, threats and vulnerabilities may challenge Critical National Infrastructure (CNI) such as healthcare and financial services, power plant systems, and supply chains, undermining a nation's economy and security.

The unexpected grounding of the 400 metre-long container ship MV Ever Given in the Suez Canal on 24 March 2021, was a great reminder that our world, and especially its supply chain, is highly interconnected and extremely fragile from incidents happening globally, regardless of borders and sectors.[8] Although oceans and seas cover more than 70 % of the Earth's surface, providing international shipping and global commerce with great levels of freedom of navigation and manoeuvring, a high wind was capable of wedging one of the world's largest container ships in one of the world's most significant sea-lanes, causing a colossal traffic jam of ships along the seaway.

The above incident demonstrates the fragility of contemporary sea lines of communication due to the presence of bottlenecks and over-reliance on just-in-time deliveries. These bottlenecks are well known and

carefully managed to optimize traffic flows and minimize traffic disruptions. But, a few maritime trade chokepoint can become one of the most significant physical characteristics of the maritime domain for human activity when an unexpected incident significantly disrupts traffic flows.[9] These areas are of prime strategic importance to the global economy, military operations, and security challenges. Even short closures of such bottlenecks threaten severe disruptions.

Such chokepoints exist in the three traditional warfighting domains (air, land, maritime) as well as in the newly established Space and Cyberspace domains. Even a single vulnerability can put a broad spectrum of a domain's activities under high pressure,

MV Ever Given blocking the Suez Canal on 24 March 2021.

undermining NATO commanders' freedom of manoeuvring and speed of action.

1.3 The Cyberspace Domain

The warfighting domain that has broadened the concept of manoeuvre, adding new dimensions to the principle and shifted further military thinking, was the introduction of cyberspace. As an artificial information domain, cyberspace is the first and only man-made domain with unique characteristics. Specifically, 'cyberspace is a fluid environment of constant contact and shifting terrain. New vulnerabilities and opportunities continually arise as the terrain changes.'[10] Its complexity derives from the fact that cyberspace not only overlaps, intersects, and engages with the four other warfare domains (air, land, maritime, space), but it is also omnipresent within every layer of our society and everyday activities.[11]

Cyberspace is a global domain within the information environment. It consists of the interdependent network of information systems infrastructures, including the Internet, telecommunication networks, computer systems, and embedded processors and controllers. Similar to aviation, which utilizes the properties of air and its dynamics, cyberspace utilizes electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.

Cyberspace is not limited only to the Internet. Even networks and devices not connected to public or open environments can become potential targets. The most well-known example is Stuxnet in 2007, where centrifuges in an Iranian nuclear enrichment plant were manipulated to randomly malfunction despite these systems being 'air-gapped'.

'Air-gapped' systems are physically isolated from less secure networks and are widely used in critical industrial environments and in military systems. While this physical separation increases the level of difficulty, it does not make them immune to new attack methods and vulnerabilities. For example, security researchers

'…anyone relying on and using cyberspace in the conduct of their activities finds themselves on the frontlines of cyberspace.'

have recently demonstrated that computer data cables could be used as wireless antennas to leak data out of air-gapped systems using radio signals emitted by the cables during read/write operations on hard disks.[12]

Cyberspace has some unique characteristics, which differentiate it significantly from all other warfighting domains. These characteristics will be explored in greater detail throughout this paper but in short, cyberspace offers an attractive and relatively inexpensive means to deliver asymmetric effects against an adversary in both times of peace and times of war. During conflict, NATO's adversaries will seek to project power and create effects in and throughout cyberspace for their military objectives, posing significant threats to the security of the largest military Alliance and its member states.

Not only state actors but also non-state actors like cyber criminals, terrorists, hacktivists, and insiders can develop new toolsets or reuse known Tactics, Techniques, and Procedures (TTPs), to influence, disrupt, and corrupt Alliance operations and missions. If a modern decision-making cycle that relies on cyberspace is not based on an effective and resilient Command and Control (C2) structure, military operation in any domain cannot be trusted to remain synchronized and conducted as planned since it can be assumed that a savvy threat actor will inescapably try to interfere with the C2 in some ways via cyberspace. Malicious activities such as terrorism, espionage, subversion, sabotage, and criminal activities may occur below the level of armed conflict and still achieve geopolitical, economic, and military objectives.

Therefore, to ensure mission success, Cyberspace Operations (CO) must not only protect the Information Environment by defending information and systems against adversary interference but must also be capable of challenging adversaries in the same way. CO apply cyberspace capabilities to create effects that support operations across the physical domains (land, air, maritime, space) and preserve friendly freedom of action in cyberspace to achieve the commander's objectives.

1.4 Manoeuvring in Cyberspace

In cyberspace, manoeuvre can be regarded as the methods and processes employed to attack and defend systems and information resources, as they give one actor a competitive advantage over another.[13] Cyberspace manoeuvre focuses on the warfighting function of manoeuvre within and throughout cyberspace to achieve physical, technical, cognitive, positional, and temporal advantages with respect to the enemy.[14]

Cyberspace manoeuvre elements, utilizing sophisticated technologies and advanced protocols, have the ability to compromise, capture, degrade, deny, or even destroy systems and networks that were once considered secure. Information of national and military significance may be manipulated using deception, decoying, conditioning, spoofing, falsification techniques, or even exfiltrated and turned against its original creator. As the technologies underlying cyberspace are constantly evolving, so too must the various cyberspace manoeuvre techniques be creative and adaptive to the new challenging operational environment. Attackers and defenders in cyberspace must constantly change their tactics and procedures to achieve cyberspace's theoretically unlimited operational reach.

No single technique can work in all scenarios and circumstances, no matter how successful it might be. Countermeasures, protective controls, and workarounds (zero-day patches, intrusion detection and prevention systems, multi-factor authentication, firewalls, etc.) are developed and implemented almost instantaneously, requiring immediate action and flexibility.

'Cyberspace is not limited only to the Internet. Even networks and devices not connected to public or open environments can become potential targets.'

Identifying and fixing one's own network vulnerabilities while identifying and exploiting vulnerabilities on the adversary's network requires a shift towards a proactive operational approach. Among the dozens of manoeuvre actions and techniques that can be used by commanders in offensive and defensive operations, are 'ambush manoeuvres', 'stimulating/probing response actions', 'distract and delay techniques', 'leverage deception practices', 'countering an asymmetric advantage', 'projecting invincibility', 'creating a false sense of security', 'social engineering mechanisms', and 'changing the terrain' methods by moving target defences.

Manoeuvring in cyberspace is less intuitive than in a traditional warfighting domain. This stems from the fact that we have been exposed to physical activities and interaction in the physical world as we grew up that have helped us develop an intuitive understanding of the traditional warfighting domains. For example, we learned the basic principle of cover and concealment while playing hide and seek with our childhood friends. However, few of us were exposed to comparable experiences in the cyberspace domain. Therefore, to understand manoeuvring in cyberspace an introduction to basic cyberspace fundamentals is necessary to level-up our appreciation of this space.

1. The American-Canadian author William Gibson conceived the word 'cyberspace' in his 1982 story, 'Burning Chrome', published by Omni magazine. Later the word would be popularized in his novel 'Neuromancer' in 1984.
2. Britannica, https://www.britannica.com/topic/cyberspace (accessed 19 July 2022).
3. John Perry Barlow was a political activist and founder of the Electronic Frontier Foundation, an international non-profit digital rights group in California.
4. New World Encyclopedia, https://www.newworldencyclopedia.org/entry/Cyberspace (accessed 19 July 2022).
5. P. MacKenzie, 'NATO Joint Air Power and Offensive Operations', JAPCC White Paper, https://www.japcc.org/white-papers/nato-joint-air-power-and-offensive-cyber-operations/ (accessed 19 July 2022).
6. S. Applegate, 'The Principle of Maneuver in Cyber Operations', CCD COE, 4th International Conference on Cyber Conflict, 2012, https://ccdcoe.org/uploads/2012/01/3_3_Applegate_ThePrincipleOfManeuverInCyberOperations.pdf (accessed 19 July 2022).
7. A. Schoka, 'Training Cyberspace Maneuver', Small Wars Journal, 2018, https://smallwarsjournal.com/jrnl/art/training-cyberspace-maneuver (accessed 19 July 2022).
8. B. Gates, 'Reasons for optimism after a difficult year, GatesNotes, 7 December 2021, https://www.gatesnotes.com/About-Bill-Gates/Year-in-Review-2021 (accessed 19 July 2022).
9. JDP 0-10, 'UK Maritime Power', Ministry of Defence, 5th Edition, October 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/662000/doctrine_uk_maritime_power_jdp_0_10.pdf (accessed 19 July 2022).
10. CCD COE, 'Cyber Commanders' Handbook', 2020, p. 14.
11. Ibid. 7.
12. B. Toulas, 'Air-gapped systems leak data via SATA cable WiFi antennas', BleepingComputer, 19 July 2022, https://www.bleepingcomputer.com/news/security/air-gapped-systems-leak-data-via-sata-cable-wifi-antennas/ (accessed 19 July 2022).
13. Ibid. 6.
14. P. Allen, 'Cyber Maneuver and Schemes of Maneuver', The Cyber Defence Review, 18 November 2020, https://cyberdefencereview.army.mil/CDR-Content/Articles/Article-View/Article/2420121/cyber-maneuver-and-schemes-of-maneuver/#:~:text=The%20scheme%20of%20maneuver%20includes,to%20specific%20actions%20and%20fires (accessed 19 July 2022).

CHAPTER 2

Cybersecurity and Cyber Defence Fundamentals

To appreciate the nuances of FoM in cyberspace, it is important to understand some basic fundamentals of cybersecurity and cyber defence. This chapter will introduce the reader to basic principles applied in cyberspace.

2.1 The CIA Triad

Confidentiality, Integrity, and Availability (CIA) are at the heart of cybersecurity, commonly referred to as the CIA triad. The triad was introduced in 1977 in a US National Institute of Standards and Technology (NIST) publication.[1] The CIA triad is the foundation upon which cybersecurity and cyber defence can be built. Similar to any other foundation, if it is poorly constructed or neglected over time, it has the potential of bringing the entire apparatus down with little to no effort from an adversary.

It is also possible to assess the CIA triad from the adversary's point of view. Confidentiality, integrity, and availability can be considered three simple yet distinct attack surfaces to be exploited to disrupt, degrade, or destroy an adversary's FoM in cyberspace. Therefore, it is essential to understand the purpose of each element of this triad and to appreciate its significance to ensuring FoM in cyberspace.

2.1.1 Confidentiality

While the importance of the CIA triad in a military activity is self-evident, confidentiality is often the most challenging objective to achieve in cyberspace. There are three main reasons for this.

Firstly, technological advances, as well as research and development in the field of cryptography, constitute an arms race in itself. Cryptanalysts attempt to use the latest technological advances, along with novel mathematical algorithms to break existing ciphers. Cryptologists continually research and develop new algorithms to remain ahead of the cryptanalysts. Therefore, ciphers rarely last more than a few decades, and their demise can sometimes be sudden and unexpected.

Take the Data Encryption System (DES) algorithm adopted by the United States National Security Agency (NSA) in 1977 for example. The DES was a tool used in unclassified and sensitive communication by both the US Government and the public. DES was upgraded in the 1990s to the triple DES (3DES) standard. It had gained widespread usage in the private sector, especially in the financial sector and credit card processing industry.[2] 3DES was also implemented in government and private sectors' computer systems, playing critical roles in Microsoft servers and Wi-Fi networks before the vulnerability of this cipher were revealed in 2016.[3] Security researchers demonstrated that it was possible to break a DES cipher key in 15 days using a commonly available $1000 computer graphics card.[4] 3DES was only a marginal improvement to DES and therefore, also vulnerable.

The cryptological arms race is becoming more pronounced with advances in fields such as AI and quantum computing, and is poised to radically transform cryptography and cryptanalysis.

Secondly, even when a good cipher exists, there are always implementation challenges. Software developers have been known to make mistakes that weaken a cipher or make a cryptographic application vulnerable to attack. One of the most notorious case, nicknamed 'Heartbleed', involved a trivial coding error that affected millions of devices on public and classified networks worldwide.[5] Most commonly though, the deployment and employment of cryptographic appliances significantly increases the complexity of a network. On occasion, this has resulted in technicians accidentally or intentionally disabling encryption while trying to troubleshoot problems.

Finally, encryption must be applied consistently throughout the infrastructure to limit the possibility of a data spill. For instance, an email between two classified laptops might be encrypted as it traverses the network (known as data in transit). Still, suppose the laptop's hard drive is not encrypted. In that case, the email could be recovered by an adversary who manages to gain remote or physical access to one of the laptops because the data is not also encrypted on the device itself (known as data at rest).

Therefore, cyber defenders must pay close attention to the cryptographic suites utilized in their environment. Not only to make sure that it is used consistently throughout the environment but also to make sure that it remains resistant to the most recent cryptanalysis attacks and free from coding defects that could make it exploitable.

2.1.2 Integrity

Integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle.[6] In other words, protecting the data so that it cannot be modified in an unauthorized or undetected manner.

Several approaches can be utilized to assure data integrity. Encryption, in addition to protecting communication from eavesdropping, is an essential tool to ensure that an adversary does not intercept data in transit with the intent of modifying it before arriving at its final destination. It also prevents an adversary from modifying encrypted data at rest.

Operating systems supported by various software packages are also used to prevent unauthorized changes to data. There are too many solutions to enumerate in this paper, but suffice to say that the principle of defence in-depth must apply to ensure that an adversary cannot easily modify data, even if it has managed to gain some degree of unauthorized access to it.

One emerging technology worth mentioning is the advent of blockchains. Well known for its use in

cryptocurrencies such as Bitcoin, and more recently, non-fungible tokens (NFTs), blockchains can also be applied to track and validate changes to data sets.[7] One such example is inventory management. It is easy to imagine the damage that an adversary could cause if it managed to falsify the database of a weapons arsenal. Blockchains offer the means of safeguarding the integrity of this invaluable data by keeping a ledger that cannot be falsified.

In this interconnected world, we must also consider the integrity of data fed into automated systems. Few systems work completely independently anymore. Flight planning software may rely on external sources of data for weather, NOTAMs (Notice to Air Missions), and maps. Most of these data sources will likely fall outside the zone of responsibility for the cyber defender responsible for defending the flight planning system. Therefore, it is impossible to find out if a threat actor may have manipulated the data being pulled by the flight planning software. This data might be manipulated to mislead the flight planning software and its operator. Alternatively, it might have been manipulated in such a way as to allow the attacker to either disable it entirely or enable the attacker to establish a persistent presence into the flight planning system and thus act as a beachhead for further compromises.

Cyber defenders need enhanced integrity checking and behavioural anomaly detection capabilities to counter these threats. Moreover, as many of these attacks can be executed in mere seconds, the use of AI to quickly analyse and automatically respond to threats will become increasingly indispensable to help maintain the integrity of any system.

2.1.3 Availability

From the system operator's point of view, availability is usually the most essential part of any information system. Whenever a system is incapable of accomplishing its function within the time and precision parameters expected, the operator's mission is impacted or outright denied. Therefore, tremendous pressure is applied against the organization responsible for the system's proper functioning.

System availability is an obvious target for any adversary. However, availability can have an even greater insidious impact than usually perceived by the operators and maintainers of the system, as it is difficult to quickly ascertain the cause of a problem whenever the system is unavailable. It may be a system malfunction, hardware failure, operator or maintainer error, malicious activity, or any combination of these. Regardless of the root cause, the technician's objective is restoring the system to a mission-capable state ASAP. However, this can lead to personnel taking shortcuts to return the system to operation. Such shortcuts are usually taken at the expense of the other two elements of the CIA triad, such as disabling encryption to facilitate troubleshooting or disabling system integrity checks to implement rapid changes without having considered second-order effects or fully understanding all the implications to confidentiality and integrity.

Restoring a system at all costs should never be the directive of an operational commander to their system maintainers. Not only does this risk introducing greater confidentiality and integrity vulnerabilities into the system, which may pose a more significant threat to the overall mission, but this might also have been the attacker's intent in the first place!

Instead, operational commanders must develop a more resilient approach that includes operating without the faulty system for extended periods through the use of backup systems or transferring this particular mission to an adjacent unit whose systems remain unaffected. In other words, information systems can and eventually will suffer battle damage (kinetic or non-kinetic). As is the case with any weapon system in the traditional warfighting domains, a military commander must ensure resiliency and redundancy are organically built-in or factored into his planning.

2.2 Cyberspace Situational Awareness

Once the CIA foundation has been laid, it is necessary to understand the environment itself and how each element (both internal and external) interact with each other to ascertain if this is a legitimate

interaction or something that emanates from adversary activity. However, SA must not be constrained only to the current situation; instead, SA should be defined as the pre-determined, current and predictive knowledge of the environment upon which operations depend, as well as factors, activities and events for friendly and adversary forces.[8]

Therefore, SA demands an understanding of each part of a system , their importance, and the interactions between these parts. Literature also shows that SA is difficult to achieve from a technical perspective; cyberspace is complex, extensive, and difficult to bound.[9] The US Joint Publication 3-12 introduced the cyberspace layer model to assist in the planning and execution of cyberspace operations.[10] The model explains how cyberspace SA must transcend three interrelated layers (Physical, Logical, and Cyber-Persona) of cyberspace (see Figure 1), making it very difficult to depict cyberspace SA in a two-dimensional manner similar to what a commander of conventional forces would be familiar with, such as a Recognized Air Picture.

Work is still ongoing on developing a cyberspace common operating picture, and various organizations and militaries have developed their own solutions.

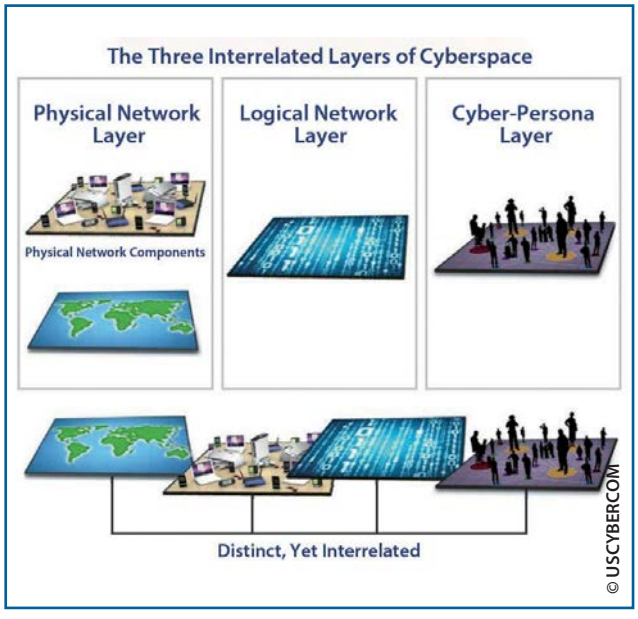


Figure 1: The Three Interrelated Layers of Cyberspace.[11]

Still, most retain a highly technical aspect that primarily serves the needs of cyberspace experts and fails to be as intuitively easy to understand as common operating pictures in the traditional warfighting domains. Meanwhile, joint operational commanders have little choice. They can either implicitly trust the explanations and recommendations their cyberspace SMEs (Subject Matter Expert) or set aside a non-negligible amount of time in their professional development to learn aspects of the cyberspace domain.

2.3 Cyberspace Risk Management

Risk Management is identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives and deciding what countermeasures, if any, to take in reducing risk to an acceptable level based on the value of the information resource to the organization.[12]

There are various methods available to assess and mitigate risks, and it is not the intent of this paper to differentiate or try to identify which method is the best as this is highly dependent on the environment and particularities of each system. However, it is important to note that risk transcends all three layers of cyberspace. Therefore, it is likely that more than one method will be required to thoroughly assess risks and select the most appropriate mitigation measures, some of which will only be effective against specific threats. In contrast, other methods will mitigate risks across a broader spectrum of systems but usually leaves gaps that must be addressed using other means. Hence, mitigation measures complement each other as a defence in-depth approach instead of a single solution promising to mitigate everything.

One cannot mitigate against all risks all the time and those who have tried have found it extremely onerous and ultimately unachievable. To judiciously identify and mitigate the most likely and most dangerous risks, it is therefore essential that the risk assessment be informed about the threats and supported by in-depth SA.

2.4 Cyberspace Threat Modelling

Threat modelling is often directed by cyberspace threat intelligence.[13] The purpose is to provide cyber defenders with a systematic analysis of what controls or defences need to be included, given the nature of the system, the attacker's profile, the most likely attack vectors (usually based on known or suspected attacker TTPs), and the most likely desired effect.

Threat modelling and threat analysis must not be underestimated. It is an arduous task because threat actors constantly seek to improve their TTPs and adapt quickly to new defences. Therefore, it takes years for analysts to become versed and effective, usually focusing on one threat actor (a single country or even a single intelligence service in a country in the case of first-tier state actors) and dedicating years of study to keep up with that specific threat actor's ever-evolving TTPs.

2.5 Defensive Cyberspace Operations

While constraints such as national policies, international norms, or local laws may preclude or limit offensive cyberspace capabilities, the ability to defend oneself in cyberspace is paramount given the ever-increasing number of incidents.

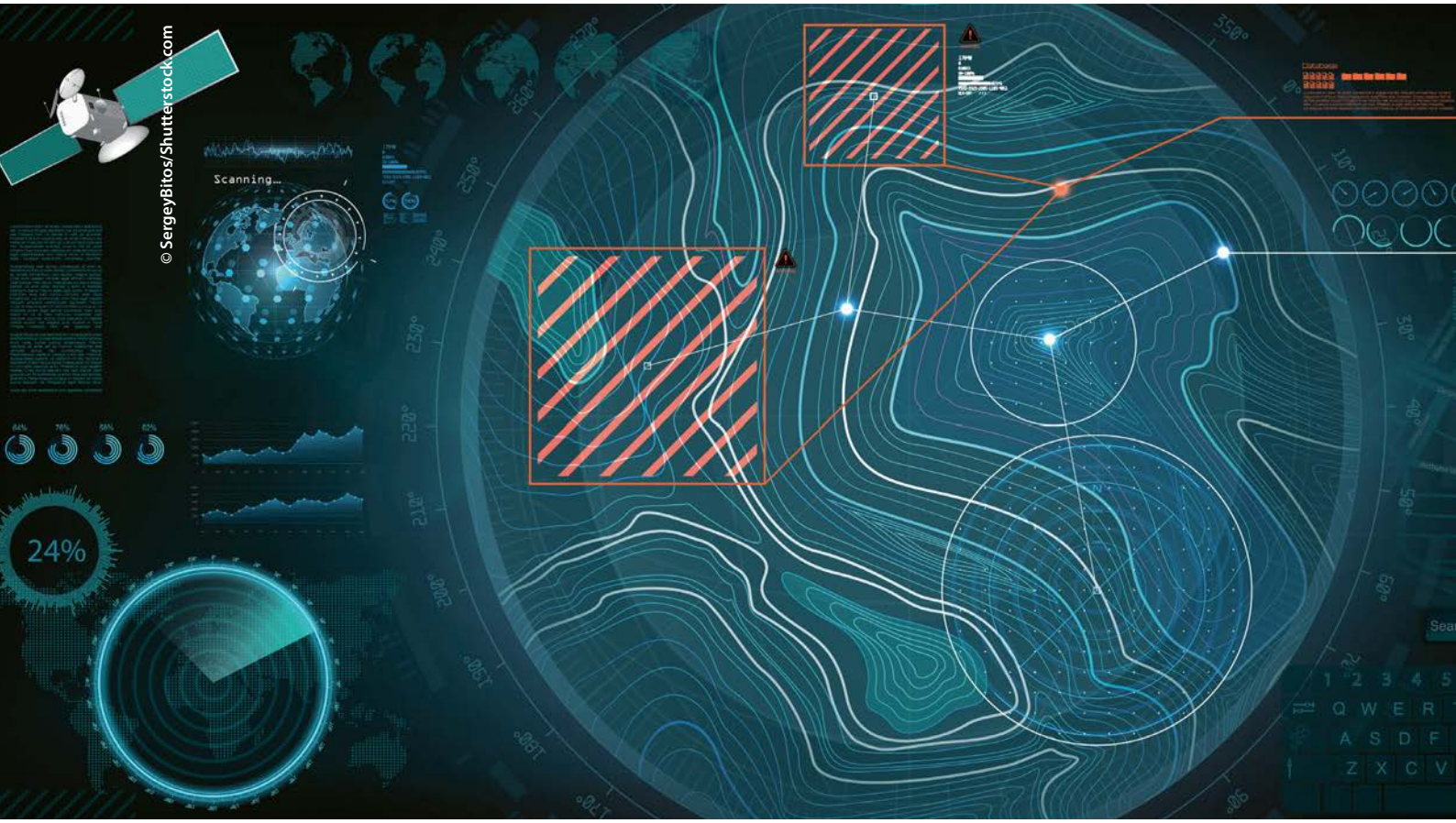
Defensive Cyberspace Operations (DCO), which are solely conducted inside the defender's own infrastructure, evolved from the NIST incident response process, which is broken down into the following steps:

- Preparation;
- Detection and Analysis;
- Containment, Eradication, and Recovery;
- Post-Incident Analysis.

There are strong similarities between this process and the area defence tactics taught in most modern army tactical schools. This is not a coincidence. The principles behind defensive cyberspace operations should be recognized as being heavily reliant on ISR to inform the detection and analysis of cybersecurity events and to ascertain whether they are a result of enemy action and how they should be handled. Intelligence is crucial to inform surveillance and reconnaissance on where to look for possible enemy activity. Surveillance is conducted using Security Information and Event Management (SIEM) tools and other sensors, whereas reconnaissance is usually carried out by teams conducting threat hunt missions, burrowing deep into systems and looking for clues that might have been left by an attacker, but which are not usually found by SIEM and traditional sensors.

One of the most significant differences between DCO and the NIST incident response process is the fact that incident response prioritizes the restoration of all systems. Concurrently, NIST enables the collection of evidence for the eventual prosecution of the attacker in a court of law. Whereas, in DCO, the primary objective is the rapid restoral of mission essential capabilities, even if this means having to cede ground (subsystems) to the adversary, or portions of systems, that are currently of lesser importance to the mission.

1. apotheon, 'The CIA Triad', TechRepublic, 30 June 2008, https://www.techrepublic.com/article/the-cia-triad/ (accessed 15 April 2022).
2. '3DES', CData Software, 2022, https://www.arcesb.com/resources/mft/3des.rst (accessed 15 April 2022).
3. R. Salz, 'The SWEET32 Issue, CVE-2016-2183', OpenSSL Blog, 2016, https://www.openssl.org/blog/blog/2016/08/24/sweet32/ (accessed 18 April 2022).
4. J. M. Gosney, '8X Nvidia GTX 1080 Ti Hashcat Benchmarks', GitHub Gist, https://gist.github.com/epixoip/ace60d09981be09544fdd35005051505 (accessed 17 April 2022).
5. J. Brodkin, 'Heartbleed developer explains OpenSSL mistake that put Web at risk', arstechnica.com, https://arstechnica.com/information-technology/2014/04/heartbleed-developer-explains-openssl-mistake-that-put-web-at-risk/ (accessed 24 August 2022).
6. J. Boritz, 'IS practitioners views on core concepts of information integrity', International Journal of Accounting Information Systems, vol 6, 2005, p. 260–279.
7. A. Hayes, 'Blockchain Facts: What Is It, How It Works, and How It Can Be Used', 24 June 2022, https://www.investopedia.com/terms/b/blockchain.asp (accessed 6 September 2022).
8. G. Conti, J. Nelson, and D. Raymond, 'Towards A Cyber Common Operating Picture', NATO CCD COE Publications, 2013, https://ccdcoe.org/uploads/2018/10/6_d1r2s4_conti.pdf, (accessed 21 April 2022).
9. J. S. Cummins, 'The Challenges Of Cyber Freedom Of Manoeuvre For Airpower In The Information Age', Joint Services Command and Staff College, 2020.
10. US Joint Chiefs of Staff, Joint Publication 3-12 - Cyberspace Operations, 2018, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (accessed 7 July 2022).
11. Ibid.
12. D.L. Cannon, CISA: Certified Information Systems Auditor Study Guide, 4th Edition, John Wiley & Sons, 2016, ch. 3.
13. S. Bromander, A. Jøsang, and M. Eian, 'Semantic Cyberthreat Modelling', Proceedings of the Eleventh Conference on Semantic Technology for Intelligence, Defence, and Security, STIDS 2016, Fairfax, VA, USA, 14–17 November 2016, http://ceur-ws.org/Vol-1788/STIDS_2016_A03_Bromander_etal.pdf, pp. 75–78.



CHAPTER 3

The Cyber-enabled OODA Loop

3.1 The Genesis of the OODA Loop

The OODA loop is a concept introduced by USAF Colonel John Boyd in his 1976 essay: Destruction and creation.[1] He applied the concept to the combat operations process, often at the operational level during military campaigns. The approach explains how agility can overcome raw power in dealing with human opponents and describes it in terms of 'competitive decision cycles [where] victory is achieved when one side is able to understand what is happening and act faster than the other'.[2] The OODA loop has also become an important concept in business[3] and law enforcement[4], and it is especially applicable in cyberspace.[5]

Military commanders and their staff have sought to accelerate their own OODA loops, following Boyd's assertion that whomever could recursively loop through it, act and then most rapidly adapt to changes on the battlefield is most likely to win.

3.2 Automated Processing at the Service of the OODA Loop

The rise of automated data processing systems (i.e., computers) ushered in the promise of an era where the OODA loop could be spun at ever-faster speeds. Early developments in information technologies gave an edge to military commanders. For example, early

radar systems in WW2 could detect and track aircraft before they were visible to the naked eye. Furthermore, a single radar system could cover a vastly larger area of the sky than any military unit could, with far fewer men. Moreover, it was able to relatively quickly enable the radar operator to assess the size of the raid and estimate their current flight path. Augmented with some human analytical thinking, it became possible to predict the likely target of the enemy aircraft and warn potential targets; mount some defence far more effectively than using the older technique of air patrolling and human lookout outposts.

Most of the early solutions that helped accelerate OODA loops were somewhat stove-piped. At some point, a human being was required to read the automated system output and decide if it should be passed along the information pipeline to the next process in the OODA loop. Therefore, the next logical step was to develop inter-process communication, the means by which a specific process output could be automatically transferred to the next automated process in the chain without the need for human interaction. This gave rise to computer networking, the Internet and what has come to be known today as cyberspace. There might always be processes requiring human interaction for a variety of reasons. To direct and tune sensors, augment or validate the analysis, decide on the most appropriate course of action, produce/issue/approve orders, manoeuvre forces on the battlefield, etc. However, it is clear that any slight improvement to help (or even completely automate) such human tasks can accelerate the OODA loop to stay ahead of the adversary's own OODA loop.

That is not to say that the Internet and cyberspace were invented exclusively to support military objectives and a faster OODA loop. Instead, it is important to note that automated data processing systems and their recursive evolutions into networked computers, the internet and cyberspace have been greatly motivated by humans seeking a competitive advantage, be it in military operations, business endeavours, or a myriad of other endeavours. Humans have always sought to automate tasks thereby concentrating on those tasks that should only be accomplished by a human operator.

This paper focuses on FoM in cyberspace in the military operation context. However, it is possible to draw parallels in all other fields of human endeavour where humans compete to gain some form of competitive edge.

3.3 Threats and Opportunities

As with any endeavour where humans compete, one must consider external threats. This existed even before the advent of cyberspace. Encryption, for example, has existed for thousands of years. Julius Caesar used simple encryption to prevent his most essential communications from being easily intercepted. This simple method helped ensure that his adversaries could not easily penetrate his OODA loop by preventing them from glimpsing the intelligence Caesar had access to. His orders to his subordinates remained cloaked from his enemies until they became visibly apparent on the battlefield.

The advent of information technologies not only played a crucial role in accelerating the OODA loop, but also as a means of disrupting one's enemy. The British made extensive use of computers in WW2 to decode Nazi communications. In effect, inserting themselves between the 'decide' and 'act' portions of the OODA loop to discover what the Nazis were planning and to respond appropriately to minimize casualties and increase operational success. Such advances played a crucial role in the war and were credited with shortening the war by two to four years.[6]

As cyberspace is maturing, it is also constantly growing in size. As of this writing, cyberspace is estimated to contain billions of devices such as computers, servers, routers, switches, smartphones, Internet of Things (IoT),[7] along with over half a million miles of undersea cables[8] and countless wireless links. Not all of these devices are directly connected to the Internet. Yet, interconnectivity permeates cyberspace, with millions of connections being set up and torn down daily. Unmanned Aerial Systems, surveillance cameras, radar signals, radios, etc., all feed one system or another, with more being added

every day. As more sensors are added to a system, this adds fidelity and helps enhance their respective OODA loop. However, with more increased inputs comes increased complexity and an exponentially growing attack surface.

To this day, militaries worldwide continue to seek advances in cyberspace in fields such as Machine Learning (ML), AI, quantum computing, quantum communication, etc., to help them run their OODA loop faster than their adversary does. They also instinctively understand that an adversary's OODA loop is a strategic target. Any disruptions levied against it, even if minuscule, might slow it down enough and for just long enough to ultimately gain the upper hand and achieve their objective faster than their adversaries.

The trick then is not to obliterate your adversary's OODA loop permanently. All that is required is to ensure that your own OODA loop remains unimpeded and able to run faster than an adversary's OODA loop long enough to win. This is accomplished in two simple and mutually supporting ways:

- Protect your own OODA loop and make it spin faster than the enemy.
- Disrupt your enemy's OODA loop sufficiently to make it slower and less reliable than your own.

This can be accomplished by leveraging the CIA triad as an attack surface as was explained in the previous chapter.

3.4 The CIA Triad in the Context of the OODA Loop

To defend one's OODA loop, one can rely on basic principles of Cyber defence: the CIA triad introduced in the previous chapter. *Confidentiality, integrity and availability* represent the three basic attack vectors by which an adversary might seek to negatively affect a computer system or network, which could markedly influence an OODA loop.

The first vector of attack is against *confidentiality*. This is the approach taken by the allies against the Nazi Enigma encryption mechanism. The main advantage of this attack vector is that, if executed savvily, it can remain undetected by the victim. This makes it the most insidious vector by affording an advantage to the attacker for a longer period than the other attack vectors and for as long as the victim remains unaware. In today's cyberspace, attacks against data and system confidentiality is the realm of cryptologic agencies such as the NSA.

'The trick is not to obliterate your adversary's OODA loop permanently. All that is required is to ensure that your own OODA loop remains unimpeded and able to run faster than an adversary's OODA loop long enough to win.'

The second vector is *integrity*. This is where the victim's data or processes are altered to modify an outcome. This can also be carried out covertly if the changes are subtle enough to escape detection. For example, a fighter jet's engine software configuration could be altered to burn more fuel, effectively reducing its patrol time (or increasing its Infrared signature) while depleting fuel reserves faster than necessary. Eventually, even the most covert integrity attacks will be discovered. If the effect to be achieved only needs to be short-lived, then an integrity attack can be more readily apparent because its discovery is unimportant. For example, the deletion of all enemy tracks on a radar tracking system. Although it might be quickly apparent to the operator that something is wrong with their system, the operator may not have time to investigate the issue and switch to a backup system. Alternatively, the problem might only be discovered after the enemy has revealed itself in other ways, such as successfully carrying out its attack.

Attacks on integrity can also create kinetic effects in addition to cyber effects. By altering data in and out of Industrial Control Systems, it is possible to damage and even physically destroy equipment.[9]

The third attack vector, *availability*, will be most readily apparent but may still take time to investigate. System availability is always foremost in the minds of system operators because they are the ones that have the most discernible, tangible, and timely impact. Therefore, it is usually the attack vector used last by cyberspace actors during a conflict. Furthermore, this is the one vector that can also be achieved via kinetic means to attain a cyber effect. The physical destruction of an undersea cable is as effective at disrupting communications between two nodes as is a cyberattack on the routers attached at one or both ends of that same undersea cable.

There is, however, a relatively large access barrier that an adversary must overcome to cause mayhem on their enemy's OODA loop. System administrators are cognizant of these attack vectors, so they have taken steps to defend them using the risk management techniques and threat modelling described in the previous chapter. Some systems are considered 'independent' from the Internet. However, it can be argued that very few systems nowadays are completely isolated. While a classified computer network may be impervious to a confidentiality attack because of military-grade encryption, it may still rely on commercial undersea cables or commercial satellites to route traffic between two distinct locations. It might also rely on commercial utilities for power and cooling. A modern fighter aircraft may depend on maintenance records and parts sourced through the Internet via one contractor and innumerable sub-contractors whose own security precautions may not be as robust as its military client. It is unlikely that contractors have the resources to ensure that any incident with a sub-contractor is prevented from putting their ability to operate their logistics chain to support military aircraft at risk. Therefore, a modern OODA loop cannot be guaranteed to be unimpeded at all times due to the complexity, interconnectivity, and most importantly, the inter-reliance between seemingly independent and physically separated systems.

3.5 Data Integrity Challenges in Evermore Complex OODA Loop

As OODA loops become increasingly automated and connected, the system of systems that is a modern OODA loop will become a figurative ocean of data. Therefore, it is essential to detect and discard anomalies that may have been generated by sensor error or malicious intervention. Because of the scale, this will require automation and AI. Capabilities need to be developed that can look at individual systems within an ODDA loop to identify malfunctioning parts and quarantine them before they have a chance to cause severe damage that would substantially slow down the system.

AI and automation are playing an increasingly important role in ensuring data integrity within any OODA loop. For example, AI can be used for cross-referencing various data sources to ensure that specific data points are correlated and identify erroneous data before it is ingested and processed in the next step in the OODA loop chain. AI and ML can also be leveraged together through behavioural analysis to ensure that data transferred between systems in an OODA loop, follow patterns that can be predicted based on known and previously observed behaviour. For example, take four distinct systems that are usually capable of detecting and alerting of impending and ongoing adversarial long-range aviation. Unexpectedly, two of these systems are reporting possible long-range aviation activity, while at the same time, the other two are unusually silent. In such a case, the system ought to be able to inform the decision-makers that anomalous activity has been detected and propose a course of action to either confirm or dismiss the possibility of an adversary's imminent long-range aviation action.

A recent concrete example of AI used to detect and defend against cyberthreats dates back to March 2022, when a Russian state actor uploaded malware to a shipping company in Lviv, Ukraine. The newly developed and unknown malware was labelled as suspicious by Microsoft Defender running Cloud Protection. An ensemble of AI machine learning models used a combination of signals across the client network and the cloud to block this malware at first sight anywhere in the world without any human intervention.[10] This effectively defeated a new and previously unknown threat before it could cause any damage to the shipping company's systems and data, thus avoiding what could have been a significant operational impact on this company.

3.6 The Supply Chain Threat

Few, if anything nowadays, are built by military organizations. Instead, they rely on a well-established and equipped set of manufacturers to produce and provision military equipment and hardware from boots to advanced weapon platforms. The more advanced the item, the longer the supply chain to create it and the greater the number of computers and electronic equipment required to build and operate it. When dealing with equipment using embedded computers, the hardware and software are usually designed and produced by the contractor and sub-contractors who are responsible for maintenance and upkeep, especially of the software whenever a bug or issue is discovered.

Two defining characteristics of cyberspace that are discussed in chapter 4 include speed and dynamic evolution, meaning that in cyberspace, it is frequently common to alter a system's function or improve its programming quickly. For example, a software update can be pushed to a radar system to improve accuracy. Alternatively, a patch can be uploaded to fix a vulnerability on a computer. An increasing number of systems used in military operations are commercial off-the-shelf systems or come from manufacturers with numerous sub-contractors. Many of these entities are now expected to maintain and improve not only the hardware, but also the software used by military organizations. We have entered an era where software updates, and in some instances, hardware upgrades have become a regular and predictable occurrence.

As an example where a supplier might be exploited in order to introduce a malicious effect, Microsoft releases a patch to its Windows operating system every second Tuesday of every month. The patch is then downloaded by most organizations that use Microsoft operating systems and then deploy it more or less quickly within their own organization. Knowing this, an attacker could conceivably penetrate Microsoft and use the 'Patch Tuesday' process to deploy malware to one or more targets. The idea is plausible and precisely what Russia[11] did between 2019 and 2021 when they compromised the SolarWinds software update service.[12] SolarWinds sells IT enterprise management software, which is used by hundreds of enterprises and government agencies across the world. By compromising SolarWinds, the attackers could deploy malware on numerous networks belonging to its clients, including the US

Commerce, Energy and Treasury departments and the US Department of Justice.[13]

Furthermore, unlike the traditional land, air and maritime domains, large parts of the cyberspace domain of importance to military commanders are owned and operated by the private sector. Therefore, the private sector now plays a significant role in protecting a country in times of conflict where combat spills into the cyberspace domain.[14] This places an additional burden on the tech sector to continue investing to keep pace with and outpace offensive TTPs.

As an alternate example, the manufacturer may not itself be at fault, but the process to deliver and implement the fix may be lacking. If the private sector issued a patch, but the intended victim has a relatively slow patch deployment process, the attacker could take the patch, reverse engineer it, and find the flaws the manufacturer intended to fix, then build and release malware to exploit the yet unpatched flaw against its victim. In a 2020 study, Mandiant, a major cyberthreats analysis company, revealed that 42% of all vulnerabilities were exploited after a patch was released by the manufacturer, with 12% of vulnerabilities exploited within a single week.[15] This creates tremendous pressure to deploy a patch as quickly as possible upon release. However, this is countered by the fact that patches also introduce possible risks of system downtime and must therefore be thoroughly tested by an organization before being deployed in any network to prevent accidental loss of service caused by a patch that interacts unexpectedly with any particular enterprise environment.

While approaches such as mission assurance can help reduce the threat by standardizing processes to detect and fix vulnerabilities and improve the speed of patching, this will never be perfect. A defender must be effective 100% of the time, whereas an attacker only needs success once. A determined adversary will eventually find some way in. Thus, resiliency will be an absolute necessity if a military commander can reliably depend on the OODA loop.


© Vitaly V. Kuzmin

3.7 Resilience

Future OODA loops will need to become increasingly resilient. Adversaries' intent on disrupting an OODA loop will target one or more systems within it until they are successful. Therefore, systems and processes must be built with the ability to adapt and self-heal whenever an input or a sub-process is lost or disrupted. This can be done by relying on multiple and separate sources to obtain the same data/output or by using backups or alternate sources that can be called upon when the primary source is disabled.

Ultimately, any part of the OODA loop must have built-in resilience and an ability to weather adversary

Russia claimed its SDRs to be 'the most advanced development of modern means of digital communication'.

attempts meant to disable it. We instinctively know that camouflage and armour (from paint schemes to flares/chaff and watertight bulkheads, to name only a few) increase combat survivability and these are techniques used on weapon systems across all domains. These defensive measures have been designed into the respective weapon systems from their inception based on current and anticipated future threats, and they are updated regularly to remain ahead of emerging threats. Systems and processes relying on and existing in cyberspace are no different and will require the same degree of preparation to ensure they are and continue to remain combat-ready. This will be achieved through cyber mission assurance.

3.8 CIA Triad Failures in the Russian OODA Loop – an Example from Ukraine

In 2021, the Russian defence ministry introduced a new Software Defined Radios (SDRs) with great fanfare. It was touted as a set of communication tools capable of working 'in all conditions'. However, this capability relied on local 3G and 4G cellular networks to function correctly. As the Russian army moved into Ukraine, it began destroying local cellular infrastructure, sometimes intentionally limiting the civilian population's access to reliable sources of information and sometimes accidentally through indiscriminate shelling. As a result, this equipment became unusable

and Russian military and intelligence personnel defaulted to using unencrypted phones and radio communications in an effort to continue to operate.[16]

The over-reliance on civilian 3G infrastructure and the inability of Russian Forces to build resilience in their SDRs, through both the deployment and employment of mobile cellular towers or the ability to utilize alternate networks such as satellite communications or mesh Wi-Fi, meant that the 'availability' principle of the CIA triad had been underappreciated. On the other hand, their fallback solution, which was clearly improvised, failed to consider the need for even basic confidentiality precautions.

This inability to reliably maintain secure communications using SDRs caused significant pain to the Russian military. For example, the intelligence arm of the Ukrainian defence ministry revealed that it had been able to listen in on an unencrypted call between a pair of Russian GRU (the foreign military intelligence agency of the General Staff of the Armed Forces of the Russian Federation) officers who complained during that call about their inability to communicate sensitive intelligence matters over secure means.[17]

There have also been multiple reports of Russian forces resorting to unencrypted radio communications during combat operations and Ukrainian forces using the information collected from these unencrypted Russian signals to mount ambushes where possible. When able, the Ukrainians were getting onto the Russian radio network to verbally harass Russian radio operators or play heavy metal music to disrupt Russian military communications.[18]

This is but one simple example of the CIA triad being employed in the context of an OODA loop. In truth, the number of possibilities to affect or defend an OODA loop is only limited by the attackers and defenders ingenuity and the understanding of the characteristics of cyberspace and the manoeuvre elements available to them, which is what we will explore in the next chapter.

1. T. Wetzel, 'Boyd's Work', John Boyd Homepage, https://www.colonelboyd.com/boydswork (accessed 25 April 2022).
2. L. Wells II, 'Maneuver In The Global Commons – The Cyber Dimension', 2010, SIGNAL Magazine, https://www.afcea.org/content/maneuver-global-commons%E2%80%94-cyber-dimension (accessed 25 April 2022).
3. C. Richards, Certain to Win: The Strategy of John Boyd, Applied to Business, Xlibris, Corporation, 2004, pp. 162–171.
4. S. Papenfuhs, 'The OODA loop, reaction time, and decision making', 2012, Police1 by Lexipol, https://www.police1.com/use-of-force/articles/the-ooda-loop-reaction-time-and-decision-making-fEOcXtsXFutU07cY/ (accessed 25 April 2022).
5. R. Clarke, The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats, 2019, Penguin Press., p. 81.
6. J. Copeland, 'Alan Turing: The Codebreaker Who Saved 'Millions Of Lives', BBC News, 2012, https://www.bbc.com/news/technology-18419691 (accessed 26 April 2022).
7. B. Jovanovic, 'Internet Of Things Statistics For 2022 – Taking Things Apart', Dataprot, 2022, https://dataprot.net/statistics/iot-statistics/ (accessed 9 May 2022).
8. 'Animated Map Reveals The 550,000 Miles Of Cable Hidden Under The Ocean That Power The Internet', [online video], Business Insider, 2016, https://www.businessinsider.com/global-fiber-optic-Internet-cables-map-2016-10 (accessed 9 May 2022).
9. K. Zetter, 'A Cyberattack Has Caused Confirmed Physical Damage For The Second Time Ever', Wired Magazine, 2015, https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ (accessed 10 May 2022).
10. Microsoft Corporation, 'Defending Ukraine: Early Lessons From The Cyber War', 2022, https://aka.ms/June22SpecialReport (accessed 23 June 2022).
11. Global Affairs Canada, 'Statement On Solarwinds Cyber Compromise', Canada.ca, 2021, https://www.canada.ca/en/global-affairs/news/2021/04/statement-on-solarwinds-cyber-compromise.html (accessed 8 May 2022).
12. B. Krebs, 'Solarwinds: What Hit Us Could Hit Others', KrebsonSecurity, [web blog], 12 January 2021, https://krebsonsecurity.com/2021/01/solarwinds-what-hit-us-could-hit-others/ (accessed 9 May 2022).
13. Ibid.
14. Microsoft Corporation, 'Defending Ukraine: Early Lessons From The Cyber War'.
15. K. Metrick, J. Semrau, and S. Sadayappan, 'Think Fast: Time Between Disclosure, Patch Release And Vulnerability Exploitation – Intelligence For Vulnerability Management, Part Two', Mandiant, [web blog] 13 April 2020, https://www.mandiant.com/resources/time-between-disclosure-patch-release-and-vulnerability-exploitation (accessed 10 May 2022).
16. S. Moss, 'Ukraine: Russian Military's Own Encrypted Phones Impacted After Destroying 3G/4G Towers, Allowing Comms To Be Intercepted', datacenterdynamics.com, 8 March 2022, https://www.datacenterdynamics.com/en/news/ukraine-russian-militarys-own-encrypted-phones-impacted-after-destroying-3g4g-towers-allowing-comms-to-be-intercepted/ (accessed 11 May 2022).
17. J. Borger, 'Vitaly Gerasimov: Second Russian General Killed, Ukraine Defence Ministry Claims', the Guardian, 8 March 2022, https://www.theguardian.com/world/2022/mar/08/vitaly-gerasimov-second-russian-general-killed-ukraine-defence-ministry-claims (accessed 11 May 2022).
18. 'Why Russian Radios In Ukraine Are Getting Spammed With Heavy Metal', The Economist, 28 March 2022, https://www.economist.com/the-economist-explains/2022/03/28/why-russian-radios-ukraine-war-intercepted-heavy-metal (accessed 11 May 2022).

CHAPTER 4

Manoeuvring in Cyberspace

4.1 Introduction

NATO defines manoeuvre as the 'Employment of forces on the battlefield through movement in combination with fire, or fire potential, to achieve a position of advantage in respect to the enemy to accomplish the mission'.[1] This description is equally applicable to all domains, albeit subject to unique characteristics in each. In recent years, cyberspace has been characterized by constant conflict between competitor states, non-state actors, and private enterprises. Battles rage across this domain continuously, and although they have not risen to the level of armed conflict, the outcome of many of these battles could have had significant impacts on the long-term future of the nations involved as any battle fought in the traditional domains.[2]

In these battles, all three sides of the CIA triad are contested. Systems are compromised (captured), degraded, or destroyed (logically or physically). Information of national and military significance is exfiltrated and turned against its original owners. The methods and processes employed to attack and defend systems and information resources in cyberspace constitute a manoeuvre, as they give one actor a competitive advantage over another.[3]

This chapter will consider the most relevant and unique characteristics that confer a competitive

advantage in cyberspace as described in Appelgate's paper[4] and examine how they affect manoeuvre in cyberspace. More specifically, it will focus on speed, operational reach, rapid concentration and reach, dynamic evolution, to conclude with stealth and the difficulties of attribution.

4.2 Characteristics of Cyberspace

Having a physical layer, it is possible to draw some parallels between cyberspace and the traditional aspect of manoeuvre. In that sense, personnel and equipment can be physically moved in order to position them in a manner to gain a position of power. However, cyberspace also benefits from unique characteristics that are drawn from the fact that it also extends into a persona and logical layer. For example, a system operator is able to physically travel to a remote site to log into a system in order to carry out some administrative functions. This need to physically travel may be a function of cybersecurity constraints, or it may be caused by a loss of connectivity that would have otherwise allowed remote access. Alternatively, that same operator may access the same system remotely using his administrative credentials (persona layer) and remote connectivity (logical layer) to carry out the same administrative functions, greatly reducing the time to carry out this task.

4.2.1 Speed

Speed is the most obvious characteristic of manoeuvre in cyberspace and is indicative of how quickly an effect may be observed or felt. The threat of a sudden and lightning-fast attack is often listed as one of the greatest benefits of an attack in cyberspace. From the defender's point of view, an attack may appear almost instantaneous and therefore achieve surprise. However, it is vital to understand that from an attacker's point of view, the attack's reconnaissance and staging phase may have taken several days, months, or even years. Therefore, while the speed of execution may appear to provide an advantage to the attacker, the time it takes to mount this attack can provide the astute and well-resourced defender with many opportunities to detect and counter an attack before the intended effect is delivered.

4.2.2 Operational Reach

The interconnectedness of cyberspace and its reliance on commercial backbone infrastructure offers an almost unlimited operational reach. Should a system be 'disconnected' from the Internet, it may still rely upon encryption over commercial infrastructures such as undersea cables or commercial satellite communications to connect with far distant nodes. Alternatively, sites may rely on commercial power, including commercially sourced and maintained backup power generation, to power their 'disconnected' systems. This interconnectedness and reliance on commercial/private suppliers offer an imaginative opponent a wide array of avenues of attack.

4.2.3 Rapid Concentration and Distribution

The ability to quickly enlist an almost unlimited number of attack points is unparalleled in the traditional domains, giving cyberspace the theoretical capacity to develop instant mass. In cyberspace, there is no lengthy manufacturing process; once a piece of code is created, it can be rapidly duplicated and run on as many computers as possible. This code can replicate quickly and often automatically through vulnerable systems. It can even be distributed through provisioning services such as cloud providers, especially if its lifespan is expected to be shorter than the time it would take the cloud provider to realize that the code it is hosting is malicious. On the other hand, this also means that a defender may have access to far greater resources than originally thought to help defend himself. The same rapid expansion can be used to create decoys and honey pots, accelerate the processing of defence data, or distribute processing in a manner that will ensure continuity of operations even if one system falls prey to a cyberattack.

This distribution of processing tactic was employed by Ukraine in January 2022, which dispersed its civil and military digital infrastructure into the public cloud across many nations from its traditional data centres

in Ukraine. Most of the Ukrainian data centres were hit by kinetic strikes at the onset of the war, but because the digital infrastructure had been redistributed across the world in cloud services hosted by Microsoft, the physical destruction of the Ukrainian data centres had no ill effect on the government and military.[5] Furthermore, Ukraine was able to leverage Microsoft's organic cybersecurity and cyber-defence capabilities to help defend its digital infrastructure.

4.2.4 Dynamic Evolution

The cyberspace domain is in constant evolution. Emerging technologies, as well as the ever-growing uses of cyberspace by humankind, remain only limited by the human imagination and technological obstacles not yet surmounted by some human imagination. For example, we often forget that Web 2.0, including social media such as Facebook and Twitter, were once considered EDTs. Few could have predicted, and even fewer would have believed back then, the influence on future political landscapes social media would eventually have, let alone predict how they could be manipulated as they have been during Brexit and the 2016 US elections.[6] Therefore, it is extremely difficult to anticipate future avenues of attack, let alone future vulnerabilities. On the other hand, a method of attack that is successful today may be rendered unexpectedly ineffective by a single change in configuration or the introduction of new procedural or technical defensive measures.

4.2.5 Stealth and Length of Attribution

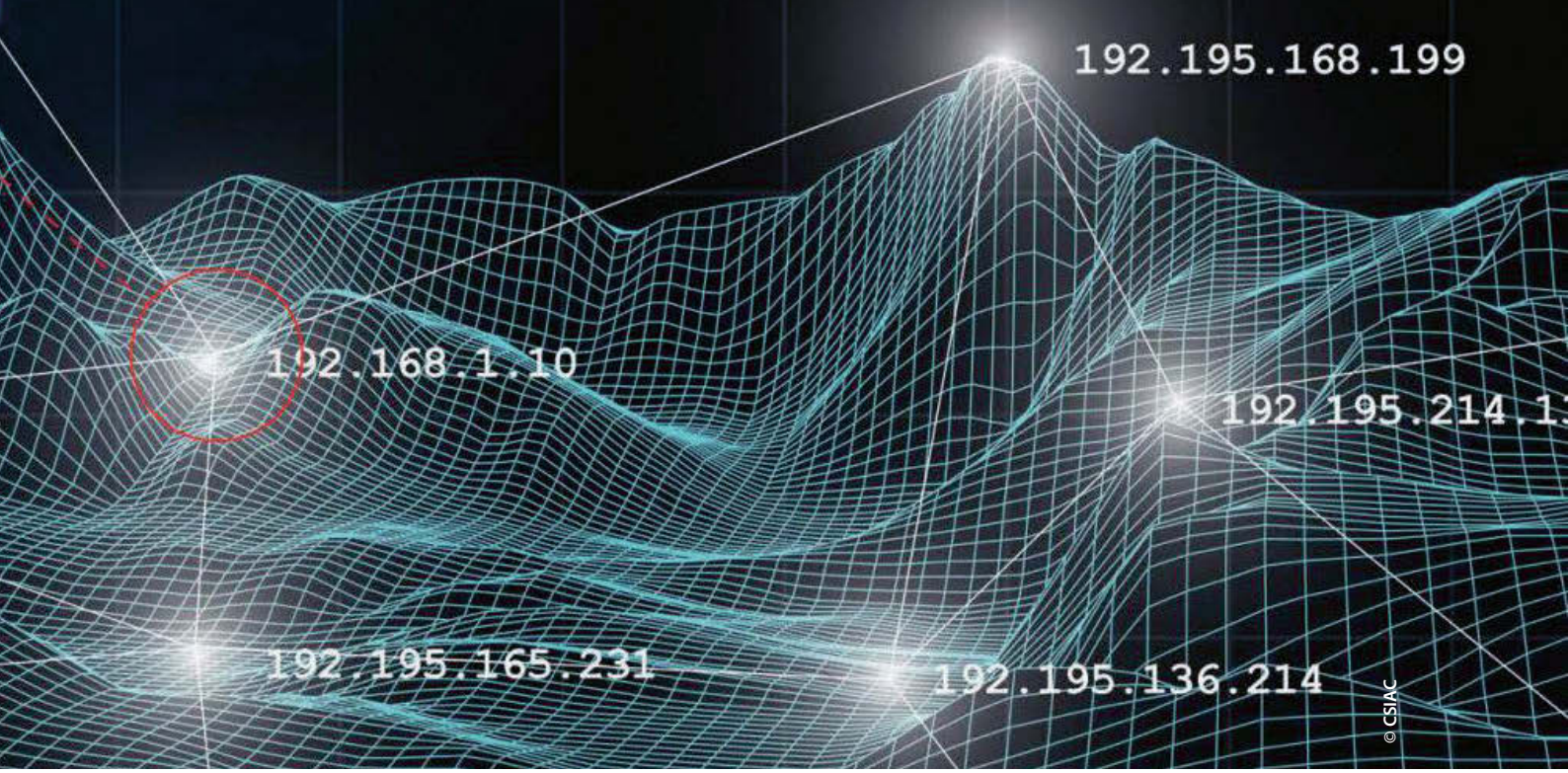
In traditional domains, it can be relatively easy to identify the origin of a lethal kinetic attack, especially if it is sustained and massive. The same is not necessarily true of an attack in cyberspace. That is not to say that an adversary can expect to remain undetected and unattributable indefinitely in cyberspace. However, a significant degree of effort is required to attribute an attack to a specific threat actor. While there have been major improvements in speed of attribution, it remains a problematic and time-consuming effort that often frustrates operational commanders seeking to find out the source of their woes.

Attribution can also be fraught with risks. A hasty attribution may fall prey to a false flag operation, whereas a lengthy forensic analysis may be too late in providing attribution to be of much use to an operational commander. Furthermore, public attribution may be unadvisable as it may reveal to the adversary the depth with which it is understood and predictable. Thus attribution could prompt the adversary to revise and improve its TTPs, making it harder for the defender to detect and counter the threat in the future.

'The means of authorization and authentication used should always be considered as the key terrain to be defended at all costs.'

Hence, an operational commander must be prepared to contend with various degrees of attribution and consider adversary effects in cyberspace in the context of the broader conflict. For example, in the days prior to 24 February 2022, when Russia was poised to invade Ukraine, a series of destructive malware programs targeted numerous governmental and private institutions within Ukraine. Microsoft's Threat Intelligence centre observed the staging of malware in Ukraine and, with the help of the US State Department, was able to assist the Ukrainian system operators in avoiding the worst of the attack.[7] While not immediately attributing the attacks to Russia, the TTPs and tools used bore a distinct resemblance to Russia's modus operandi. Undoubtedly, this subjective attribution influenced the assessment of whether or not Russia was preparing to invade.

Therefore, the greatest challenge is not so much the stealth of an attacker but instead the ability by the defender to sift through the deluge of data captured by sensors, select and analyse the most relevant data, and provide sufficiently actionable intelligence to inform commanders and other decision-makers in a timely fashion.



The term 'Terrain' is traditionally used to describe physical locations that can be easily pointed to on a map. But that reality is more complex in multi-layered cyberspace.

4.2.6 Fuzziness of an Armed Attack Threshold

International laws and norms have long been established to codify what constitutes an armed attack in the traditional kinetic domains. This is rooted in a clear understanding of geographic boundaries and sovereignty. However, the logical and persona layers have blurred these boundaries in cyberspace. Furthermore, the ephemeral and rapidly changing environment lent itself well to a generalized impression by government bodies and lawmakers that damage caused in cyberspace was reversible relatively quickly and, therefore, not that significant. At least compared to the widespread destruction and loss of life normally associated with armed attacks. Therefore, mischief in cyberspace was more often equated with criminal and civil liability than a generalized threat to a country's sovereignty and right of self-government.

Although this is now changing and many countries have taken stances in that regard and are working at codifying into international laws and norms what could conceivably constitute an armed attack in cyberspace, much debate remains on the international stage. This opened up a gap where nation states through their government agencies and/or through third parties (cyber criminals, hacktivists, etc.), have carried out offensive cyberspace operations without regard as to the potential of meaningful repercussions for having infringed still imprecise international norms and laws. This gap continues to shift faster than lawmakers can agree to legislate due in large part to the rapid and unpredictable course of the evolution of cyberspace and, by extension, the information space has undergone these last decades and continues to undergo at this very moment.

Therefore, at least some offensive cyberspace operations will continue to evolve in a space where international laws and norms lag behind and are ineffective at constraining potential cyber effects. We can expect malicious actors to challenge and contest NATO and nations FoM in cyberspace not only in times of conflict but also in times of tension and even in times of peace, as has been the case for at least the last two decades.

4.3 Cyberspace Terrain

The concept of manoeuvring implies the need for terrain to manoeuvre through. The term terrain is traditionally used to describe physical locations that can be easily pointed to on a map. Since cyberspace is conceptually made up of three layers (physical,

logical, and persona), cyberspace terrain differs from our traditional concept of physical terrain. For example, a Virtual Private Network (VPN) server might be located in a building on a college campus alongside many other servers. That is the terrain it occupies on the physical layer of cyberspace. At the logical level, that same VPN server allows students to access college resources from afar as if they were located on campus. Moreover, on the persona layer, that same student with a name and likely many online personas is recognized by a unique ID; likely their student ID number. Therefore, when manoeuvring in cyberspace, it is essential to realize that a single manoeuvre element can act in one layer, but typically transcend two if not all three layers simultaneously.

The virtual nature of cyber terrain at the logical and persona layers also makes it possible to dynamically create, modify, and destroy terrain quickly and frequently; at machine speed.[8] This provides a degree of flexibility and complexity unequalled in the traditional warfighting domains. This means that a defender (or attacker) can quickly and drastically alter the terrain to their advantage in ways that are impossible to achieve in the kinetic world. For example, a defender may decide to deploy a firewall using a cloud-based service, route-specific traffic of interest, and inspect this traffic for malicious activity. While seemingly complicated, a skilled operator can accomplish this in mere minutes and would likely interfere, deny, or roll back any progress made by an attacker.

4.4 Cyberspace Key Terrain

Considerable research has been conducted to try to define key terrain in cyberspace, and the subject remains divisive amongst practitioners. However, for the benefit of this paper, we postulate in this section that Authentication and Authorization is always key terrain for cyberspace.

In traditional, kinetic warfare, key terrain is defined as the features that provide a marked advantage to someone attacking or defending. While true at its core, it is difficult to pin down any particular feature of cyberspace terrain as Key Terrain given the dynamic nature of cyberspace and the speed with which the terrain can be altered. Not to mention the seemingly unlimited possibilities available to defenders (and attackers) in their choice of how to alter the terrain.

However, throughout all the options available to the warfighter in cyberspace, one key element consistently remains the same. To carry out any action (offensive or defensive), the warfighter must have some degree of access and authorization. To access a website, someone browsing the Internet is likely going through several layers of inspection consisting of authentication (assurance and confirmation of a user's identity) and authorization (the right or permission that is granted to a user to access/modify/interact/delete a system resource, i.e. file, process, etc.). These layers are invisible to the visitor, but they are there to ensure that the visitor's activity does not threaten the web server and its content. Before saving changes to a file on a file server, the operating system will verify that the user has 'write' permission to that file. In short, any action taken in cyberspace goes through a series of authentication and authorization steps. Any action an attacker wishes to take will require it to gain some degree of access. The attacker's objective may be easily achievable due to an error in configuration, a code error, or the inability of the defender to anticipate an attack vector. Still, in the end, the attacker had to bypass whatever authorization and authentication means are placed in its path.

Therefore, the means of authorization and authentication used should always be considered as the key terrain to be defended at all costs. Once an attacker has overcome these means, attempts at regaining the advantage by the defender will always be exceedingly costly and time-consuming.

This approach is at the centre of NIST standard SP 800-207 'Zero Trust Architecture Framework'[9] which assumes that there are no traditional network edges. It requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security

configuration and posture before being granted or keeping access to applications and data. Therefore, technology and know-how exist to secure cyberspace's key terrain. While an ever-increasing number of private and public sector organizations are implementing the zero trust framework, this will require a paradigm shift in a military context where defensive boundaries are ingrained into military thinking and strategies.

4.5 Manoeuvre Elements

Manoeuvre elements are a combination of personnel and TTPs that enable them to achieve some degree of effects and action in one or more layers of cyberspace. As is the case in traditional domains, these compositions can be extremely diverse, with personnel employing similar tactics but different tools to achieve similar results. Therefore, this chapter will focus on broad categories of compositions that can be utilized as manoeuvre elements in cyberspace. Furthermore, combining cyberspace personnel and TTPs into cross-domain 'battle groups' and further integrating them into Multi-Domain Operations (MDO) is the obvious force multiplier and its advantages will be highlighted in chapter 6. Notwithstanding that, there are many possible iterations that are well beyond the scope of this paper. As a result, it would not be prudent to try and enumerate every combination, but instead, we will focus on explaining more generic roles and potential.

4.5.1 System Management

At the core of system management is the capability to shape and alter the terrain to meet the users' needs and to defend against threats. These are system administrators, system maintainers, programmers, mission assurance specialists, and incident response specialists.

4.5.2 Surveillance

The ability to sense activity in cyberspace is as important as in any of the traditional warfighting domains. Most of the technology in cyberspace has some built-in capability to record and log activities, which provides innumerable opportunities to capture evidence of potentially malicious activity. However, the main challenge is the sheer volume of records that can be produced and the difficulties associated with storing, sorting and analysing all of this data to find potential threats hiding in the 'noise' generated by all the benign activity.

Surveillance teams quickly specialize into sub-specialties to help breakout this significant problem into smaller, more manageable pieces such as network traffic analysis or event log analysis. To help cope with such large volumes of data, analysts are assisted by automated capabilities to detect known malicious behaviour using frequently updated fingerprints, usually referred to as an Indicator of Compromises (IoC).

This field is in constant evolution and will greatly benefit from AI and ML advances to help scrutinize an ever-increasing volume of data, with the Microsoft example in section 4.2.5 having made use of AI and being a harbinger of things to come. However, end users themselves are an abundant and invaluable resource available to analysts that are continuously underestimated. End users are well placed to detect possible adversary activities and manoeuvring. Their reaction to suspicious emails or activities might be the only thing between a successful or thwarted attack. In effect, every end user can be employed as a sensor and plays a similar role in cyberspace to soldiers entrenched on a battlefield frontline. How well-trained and equipped they are will, in many cases, be the overriding factor in how the war turns out.

4.5.3 Reconnaissance

Defence in-depth is a universally recognized approach to help reduce the risk of compromise and is equally so in cyberspace. Just as a facility may augment its alarm system with patrol guards to detect unauthorized entry, the security provided by surveillance capabilities in cyberspace can also be augmented with assets capable of conducting the cyber equivalent of ground patrols.

'Hunt teams' are such an example, where cyber defenders will inspect cyberspace's physical, logical and persona layers in search of evidence of tampering. This approach may discover residue of malicious files that evaded surveillance capabilities or the presence of an unauthorized account with administrative privileges.

Another example is 'red teams', which take an outsider view and approach to test detection and response mechanisms. They will explore all threat surfaces for vulnerabilities and weaknesses and try to exploit them undetected. Red teams usually have one of two predictable outcomes. Either they are detected and the response process is exercised, or they remain undetected and thus identify shortcomings in the detection and protection mechanisms in place that are subsequently addressed.

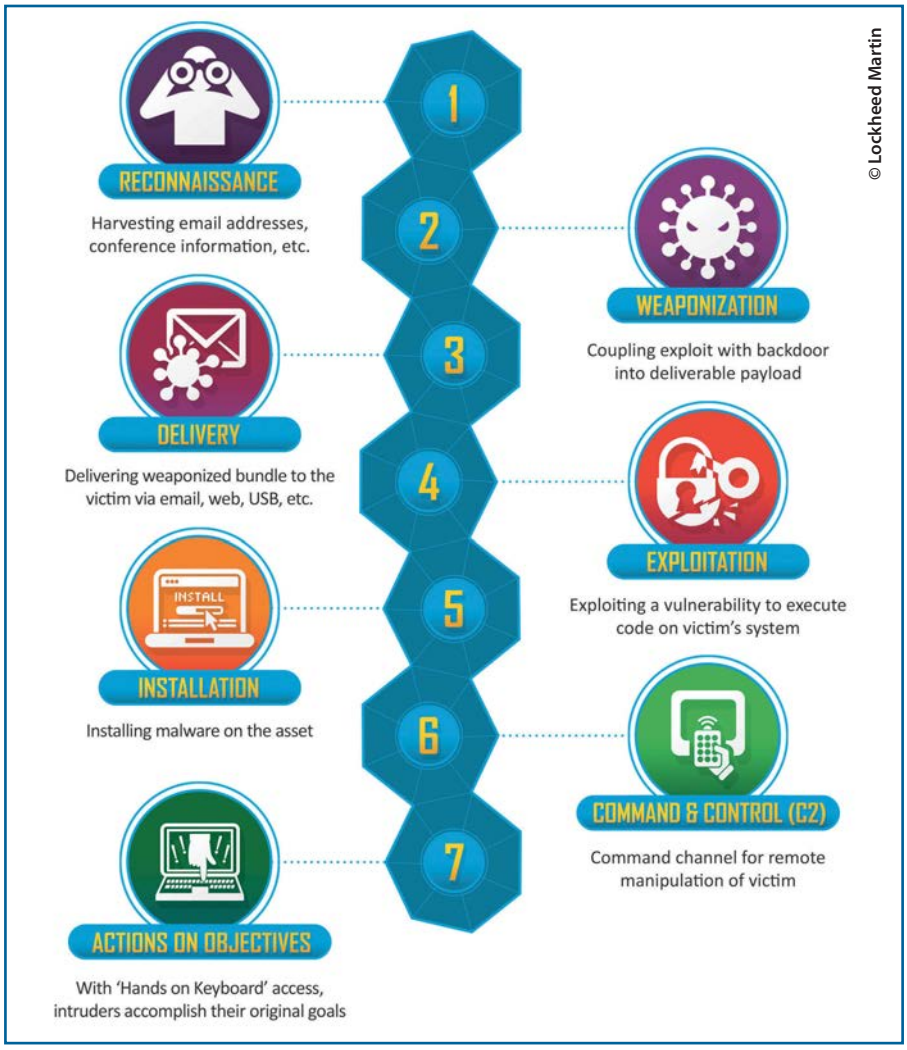


Figure 2: Lockheed Martin Cyber Kill Chain.[11]

4.5.4 Forensics

Whenever a surveillance or reconnaissance team unearths evidence of possible malicious activity, a forensic capability is called upon to help establish the ground truth. It is essential to follow the trail of evidence to discover how the adversary managed to overcome defences, where it is currently operating within friendly cyberspace, and what further action it may be about to carry out.

Forensic capabilities are indispensable to mount a counter-offensive and repel the adversary out of friendly cyberspace. It also informs surveillance and reconnaissance capabilities to help enhance their detection efforts. Lastly, it informs system management capabilities to help shore up weaknesses in defences to avoid an adversary successfully utilizing the same method of attack more than once.

4.5.5 Offensive Capabilities

A discussion on offensive cyberspace capabilities delves into other aspects of FoM in cyberspace that are well beyond the scope and classification of this paper. Suffice to say that various models of cyber kill chains have been introduced to standardize the approach taken by offensive capabilities to achieve their objectives.[10] The Cyber Kill Chain from Lockheed

Martin and the ATT&CK Framework from MITRE are the best-known examples. Both follow a sequential series of steps, implying that once a foothold is established, the cycle can be re-initiated recursively to penetrate deeper into the target organization or as a means of moving laterally to new victims with which the original victim shares privileged trust relationships.

The most important lesson to be learned from these kill chains (see Figure 2, page 31) is that with the combined help of all defensive cyberspace capabilities listed previously, it is theoretically possible to detect and respond to an adversary action at any stage of an attack. Potentially offering an opportunity to counter an adversary before he successfully delivers its effect. Or, having been able to minimize the attacker's impact by leveraging pre-planned response plans and resilience planning.

4.6 Conclusion

Manoeuvre in cyberspace is analogous to manoeuvre in the physical domains but in a more abstract way, given that it spans three layers. Manoeuvre elements operating in and through cyberspace must therefore adapt their TTPs to take full advantage of the unique characteristics of cyberspace in their effort to achieve their position of advantage over their adversary. One of the most difficult tasks for warfighters relying on cyberspace in general and for any manoeuvre element, in particular, is the need to keep up with technological advances. Failing to keep up with the adversaries technologically can jeopardize our ability to defend ourselves in cyberspace or prevent NATO and its allies from achieving their goals. Hence, the importance of remaining agile and continually assessing emerging technologies for their potential application in cyberspace operations.

1. North Atlantic Treaty Organization, 'NATO Glossary Of Terms And Definitions AAP-06', 6th ed, NATO Standardization Office, 2021, p. 81
2. J. Markoff, 'Before The Gunfire, Cyberattacks', Nytimes.com, 12 August 2008, https://www.nytimes.com/2008/08/13/technology/13cyber.html, (accessed 16 May 2022).
3. S.D. Applegate, 'Towards A Cyber Common Operating Picture', 4th International Conference on Cyber Conflict, NATO CCD COE Publications, 2012, https://ccdcoe.org/uploads/2012/01/3_3_Applegate_ThePrincipleOfManeuverInCyberOperations.pdf, (accessed 16 May 2022).
4. Ibid.
5. Microsoft Corporation, 'Defending Ukraine: Early Lessons From The Cyber War'.
6. The Great Hack, Dir. Jehane Noujaim and Karim Amer, USA, Netflix, 2019.
7. T. Burt, 'The Hybrid War In Ukraine', Microsoft Corporation, 27 April 2022, https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/, (accessed 17 May 2022).
8. D. Raymond et al., 'Key Terrain in Cyberspace: Seeking the High Ground', 6th International Conference on Cyber Conflict, NATO CCD COE Publications, 2016, https://ccdcoe.org/uploads/2018/10/d2r1s8_raymondcross.pdf, (accessed 16 May 2022).
9. S. Rose et al., 'NIST Special Publication 800-207 - Zero Trust Architecture' National Institute of Standards and Technology, 2020, Zero Trust Architecture, https://doi.org/10.6028/NIST.SP.800-207, (accessed 18 May 2022).
10. D. Van Puyvelde, and A. Brantly, Cybersecurity. Politics, Governance And Conflict In Cyberspace, Polity Press, 2019, p. 66.
11. Lockheed Martin, Cyber Kill Chain, [online image], https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, (accessed 7 July 2022).

© US Army illustration

CHAPTER 5

In the Era of Digital Transformation

5.1 Emerging and Disruptive Technologies

Knowledge development and new technologies are essential for Alliance security and operations. NATO organizations must understand the full impact of Emerging and Disruptive Technologies (EDTs) as an enabler and enhancer of operational superiority. Maintaining the technological edge in AI, ML, quantum computing, autonomous weapon systems, and other uses of technologies is vital for NATO's deterrence and defence posture.

Near-peer state actor competitors are investing heavily in disruptive technologies to impede the Alliance's military-strategic objectives. NATO must continuously improve its ability to understand the environment, decide faster, be proactive and maintain the advantage of its OODA loops. The challenging and competitive environment requires continuous adaptation and transformation, especially in the age of digitization and when considering that the norms and laws governing cyberspace are applied unequally amongst nations and often ignored by rogue nations and malicious actors.

In July 2020, NATO Secretary General Jens Stoltenberg announced the creation of an Advisory Group on EDTs to support NATO's innovation efforts and to adopt new technologies. Twelve experts across the Alliance provided their recommendations to NATO allies on how to leverage and adopt these new technologies in both the short- and long-term to sustain peace and prosperity.

'NATO's Advisory Group on EDTs has identified quantum as one of its key emerging and disruptive technologies as it has recognized the transformative potential and the geopolitical value of its applications.'

In March 2021, the Advisory Group on EDTs issued its first annual report, identifying and prioritizing seven key, dual-use, technologies that would present risks and opportunities to NATO's defence and security mission. The following areas were declared the most important technologies that NATO needs to adapt at a pace that is appropriate to the rapidly evolving EDT landscape:

- Advances in ML, AI and autonomy;
- Developments in quantum enabled technologies;
- Applications of data security algorithms;
- Computing enabled hardware;
- Utilization of biological and synthetic materials;
- Hypersonic technologies and space.

Not all areas identified by the Advisory Group are specific to cyberspace. Some, such as AI and Quantum-enabled technologies, will transcend most if not all human endeavours. Many of these areas are poised to transform cyberspace as a whole and shape cyberspace operations in particular. Therefore, they are worth more attention.

5.2 Artificial Intelligence, Machine Learning and Automation

While NATO has realized that adopting and applying these new and emerging technologies will accelerate the Alliance's digital transformation and shape the future operating environment, this can only be fulfilled within an effective cyber hygiene ecosystem.[1] Such an ecosystem will provide the environment within NATO that can experiment, train, develop and apply its competencies in EDT agility provided NATO leadership takes on the role of caretaker for its ecosystem.

Cyberspace remains crucial for the constant evolution of the digital world. The continuous defence and protection of technologies and applications in the cyber-physical space require sophisticated and autonomous cyber TTPs and strong security protocols.[2]

'AI technologies are already transforming the nature of cyberattack.'[3] Both defenders and threat actors make use of AI applications to produce attacks that are more successful. AI-powered attacks can replicate natural language, generate realistic phishing emails and develop autonomous and self-replicating malware which can propagate at a speed and scale that is impossible to prevent and stop with human effort.[4]

To keep up with the speed, scale and sophistication of automated cyberattacks, defenders have to rely on AI to identify vulnerabilities before they can be exploited and to detect malicious activity at the early stages of conflict, before an effect can be successfully achieved. Integrating AI technologies into incident response systems enables security teams to identify, investigate and remediate threats much faster.

Cyberattacks such as spam emails, Distributed Denial of Service (DDoS), Man-in-the-Middle, botnets, ransomware and malware are constantly rising in number and evolving in complexity and sophistication. To help mitigate this challenging threat landscape, the US Defence Advanced Research Projects Agency (DARPA) launched in 2015 the Cyber Grand Challenge contest to create a cyber-reasoning system capable of self-learning and operating without human intervention, finding flaws in software, formulating patches and deploying them in real time on a

network. The Cyber Grand Challenge Final Event was hosted live on 4th August 2016,[5] and only seven teams out of over 100 made it to watch their fully independent reasoning systems attack each other in the world's first fully automated capture-the-flag competition. For twelve hours, the seven teams' Cyber Reasoning Systems were scored based on their capability to protect hosts, automatically identify software flaws, scan the network for vulnerabilities, and maintain the correct function of the software. Demonstrating that it was possible, at least in controlled environments, to build intelligent systems capable of self-defence faster than it could if it required human intervention.

Automated software vulnerability analysis is a challenging process; without AI and ML, it would also be unsolvable. Autonomous attack platforms capable of discovering and exploiting new vulnerabilities can only be countered by increasingly automated defences designed with cyber resilience built-in. According to the most recent DDoS attack trends[6] – with a bandwidth larger than 250 Gigabits per second – the overall number of attacks increased by 1,300% between 2020 and 2021. Most of these attacks were based on Advanced Persistent Threats (APTs) methods, in which actors attempted multiple intrusions scattered over time. By analysing the feedback of these attempts, they try to adjust their strategy. Current widely used security technologies such as antivirus and Intrusion Detection Systems (IDS) are not capable of detecting such targeted and advanced threats. Therefore, the evolution of these technologies must include AI and ML to ensure that autonomous attack platforms do not overwhelm or outmanoeuvre them.

When designing and deploying emerging technologies in military and defence applications, it must be acknowledged that those might inherit significant security vulnerabilities ready to be exploited by adversaries. Adversarial AI applications, for instance, could poison small amounts of ML data, underpinning and compromising the accuracy and performance of the systems. To protect military applications and mission-critical systems from

AI-generated image.

sophisticated adversarial attacks, robust techniques and procedures will need to be developed.

AI-enabled technologies have the capacity to impact warfare and NATO's armed forces as they have been incorporated into a wide range of military applications, from autonomous vehicles to data processing and monitoring tools. Therefore, in October 2021, NATO adopted its first AI strategy to define the standards and create a roadmap for AI capability building and responsible use across the Alliance. It identifies six Principles of Responsible Use for AI in defence and security. These principles are:

- Lawfulness;
- Responsibility and accountability;
- Explainability and traceability;
- Reliability;
- Governability;
- Bias mitigation.

Explainability and traceability, reliability, and bias mitigation are steps in the right direction towards ensuring that AI and ML will be able to carry out their functions free from interference from adversaries. However, much work remains to be done by the Advisory Group on EDTs to concretely implement these principles into actionable solutions.

5.3 5G, Internet of Things, Big Data, and Quantum Computing

The next generation of mobile technology, 5G, is starting to dominate the civil telecommunication landscape and is becoming the backbone of society. New challenges are appearing, threatening the security and reliability of other EDTs, such as AI, ML, and big data. 5G technology not only facilitates interoperability to the Alliance, providing extremely high-speed, high-density, large-volume, low-latency, and power-efficient mobile communications, it also drastically increases the attack surface and the number of potential entry points to the networks by introducing new security challenges and risks.

5G networks enable the interconnection of various devices and sensors in the IoT landscape, accelerating the development of technologies such as Connected Autonomous Vehicles, 'smart cities', and Virtual Reality applications. IoT is described as physical objects (or groups of such objects) with sensors, processing ability, software, and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks. Its applications are countless from small weather stations providing additional data for more accurate weather forecasting models to pace makers informing doctors in real time of patient's condition. Alternatively, fridges with cameras able to detect when someone is running low on milk that is about to expire. Or a seismic sensor able to count the number of people currently in a room. Anything and everything that can be equipped with a sensor to track and report on an innumerable number of inputs can and will eventually be turned into an IoT.

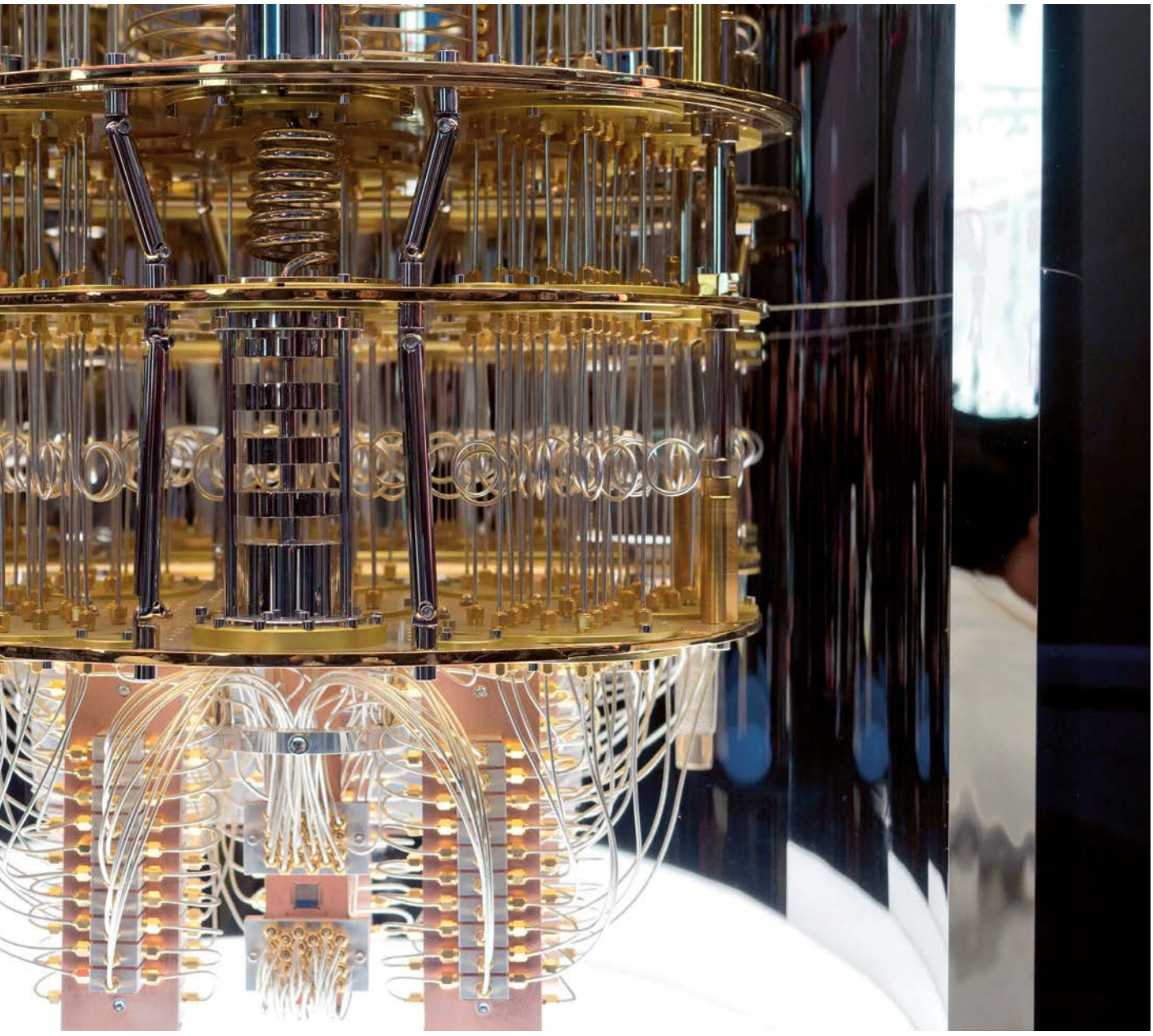
However, the increased speed brought about by 5G deployment and the number of connected everyday devices enabling connection to almost 'everything-to-everything' instantaneously and autonomously, renders any perimeter network defence ineffective.[7] It is widely reported that the number of IoT devices worldwide will almost triple from 10 billion in 2020 to more than 30 billion in 2030, expanding cyberspace's physical and digital frontiers tremendously in the future.[8]

As an example, in September 2016, a DDoS attack was launched by cyber criminals using 'Mirai' malware infecting smart devices such as IP cameras, home routers, thermostats, and digital video recorders, turning them into a network of remotely controlled bots (botnet).[9] While the intended targets of the DDoS attack were operators of a popular video game called Minecraft as an extortion scam, the additional load on the internet backbone caused a major Domain Name Server that provided services to companies such as

Quantum computer built by IBM: the IBM Q System One.[10]

Netflix, Twitter, and Airbnb to be overwhelmed and disabled. Massive machine-to-machine communications based on low-cost devices with low-security features are becoming the weakest points in the arising 5G cybersecurity landscape that promises to connect an ever-increasing number of low-cost devices in an ever increasingly fast network.

Another threat applies to the data collection and data processing within IoT and portable devices such as smartphones. Zettabytes worth of data is produced and transmitted daily, requiring increasingly robust capabilities and standardized interoperability procedures to collect, process, interpret and store data. This is commonly referred to as 'Big Data' and its complexity derives not only from volume alone but also from the speed at which those bits of data are produced and the variety of data types. A general definition of big data includes all 'information assets characterized by such a high volume, velocity and variety [that]



require specific technology and analytical methods for its transformation into volume.'[11] Big data is capable of yielding insight and understanding that far outpace any human cognitive abilities, for example by uncovering hidden patterns correlations and trends. Thus, allowing for greater precision and accuracy when making decisions.[12]

Moreover, this vast amount of data must be almost instantaneously accessible and available. Distributed computing architecture, also known as edge computing, is based on the concept that data is stored and processed at the periphery of the network, closer to the source of data. Therefore, the response times are significantly improved while also saving bandwidth.

Quantum computing is another dual-use technology that has the potential to redefine cybersecurity. Quantum computers allow more complicated computational structures leading to significantly enhanced measurements, sensing, and precision capabilities. The processing power expands at an unfathomable rate, and new forms of code and algorithms are created to leverage physical phenomena at the atomic and sub-atomic scale. This technology can enhance and accelerate ML and AI applications by introducing new concepts such as quantum sampling, quantum sensing, and quantum neural networks, based on the properties and states of matter that are more 'probabilistic' than 'deterministic'.

Quantum technologies offer tremendous potential for military applications and are capable of changing the conduct of warfare and the outcomes of battles.[13] Underground mapping techniques, early-warning systems for natural disasters, autonomous systems able to 'see' around corners, portable human brain activity scanners, quantum Positioning Navigation and Timing (PNT) devices and quantum radar technologies are just a few of the many promising technologies ready to be applied not very far in the future.

Quantum communications has the potential to transform cybersecurity. Quantum particles are particularly effective for the exchange of cryptographic keys, as they differentiate from the classical binary digit (0s and 1s) data transmission methods and instead use quantum bits known as 'qubits' (0s and 1s at the same time that probabilistically collapse into the most likely solution), enabling novel methods of cracking for the most commonly used forms of encryption protocols on the internet. The future 'quantum internet' will be an ultra-secure, unhackable network of entangled quantum computers with quantum processors and quantum Internet software applications.

NATO's Advisory Group on EDTs has identified quantum as one of its key emerging and disruptive technologies as it has recognized the transformative potential and the geopolitical value of its applications.[14]

'While NATO has realized that adopting and applying these new and emerging technologies will accelerate the Alliance's digital transformation and shape the future operating environment, this can only be fulfilled within an effective cyber hygiene ecosystem.'

The race for 'quantum supremacy' and 'quantum resistant' digital infrastructure among governments and civilian industry is already on.[15] Only recently, in July 2022, NIST announced, after six years of effort, the first group of encryption tools (algorithms) designed to withstand a possible future cryptanalysis-attack from a quantum computer. The NIST's post-quantum cryptography program has set a two year timeline to approve quantum-resistant algorithms that will lead to a standard and increase the security of digital information significantly in the future.[16]

Allied militaries must proactively engage in the research and development of the EDTs to reap the benefits of their state-of-the-art applications. NATO must become familiar with these technologies and their capabilities and actively participate in the new innovative ecosystem. Only in this way will the Alliance be able to understand the potential risks and challenges associated with the EDTs and take full advantage.

5.4 Blockchains

A blockchain is a type of Distributed Ledger Technology (DLT) that consists of growing list of records, called blocks, that are securely linked together using cryptography.[17] While mostly known globally for crypto currencies such as Bitcoin, blockchains can have many uses including smart contracts, gaming, and most interestingly for military applications in supply chain management.

The main advantages of blockchains include its distributed nature, which makes it extremely difficult for an adversary to compromise the integrity or availability of the underlying data. Additionally, blockchains produce non-repudiable records, making it impossible for an attacker to falsify records unless it can break the encryption used by the blockchain. This last point is especially important to consider as older blockchain technologies are vulnerable to quantum computing decryption attacks. Therefore, blockchains employed in military applications such as maintenance records for aircrafts or weapon ledgers must employ cryptographic algorithms that are resistant to quantum attacks.

Finally, blockchains do not provide any degree of confidentiality. Therefore, additional measures must be implemented when the data items tracked in the blockchain must be protected from unauthorized access. For example, this could be achieved by hosting the blockchain on a classified network not connected directly to the Internet.

5.5 Practical Examples of EDTs in Support of Space Domain

Space-based assets are increasingly becoming potential targets for cyberattacks as their importance and impact on modern military operations have increased exponentially over the last few decades. In December 2019, NATO decided to focus more on space, recognizing it as an operational domain and releasing a new Space Policy.

Space-based services and capabilities have become vital parts of human activities and are considered critical national infrastructures, including communication satellites, navigation systems, and weather forecasting and imaging satellites. China and Russia are investing heavily in improving their capabilities in space-based services and ground support infrastructure. Both countries have developed multiple counter space capabilities, ready to degrade and deny adversary use of space-based assets.

The weaponization of space has been facilitated not only by kinetic physical weapons, such as anti-satellite strikes but especially by the non-kinetic effects which may not reach the threshold of an armed attack, such as the growing array of cyberthreats. AI and ML enabled Cyberattacks could be executed at the speed of light, being less visible and difficult to attribute, targeting a wide range of vulnerabilities in the ground and space segments of a satellite's data links and supply chain. Electronic Warfare attacks target the link between the ground station and the satellite itself, using jamming or spoofing to interfere with radio frequency signals. Whereas cyberthreats focus on the data and the systems that transit through the link as potential intrusion path for cyberattacks to disrupt the data itself or the processors at the ground station or on-board the satellite.

Space is evolving to the next frontier for cyberspace. As cyberspace operations allow adversaries to manage the escalation of a conflict to achieve the desired conditions with minimal strategic cost and do not need significant resources, seizing 'cyberspace superiority' becomes a top priority. A cyberattack on satellites can result in data loss and widespread connection disruptions, significantly exacerbating the consequences to public safety, economic welfare, and national security due to the rise in IoT devices and 5G networks.

To mitigate cyberthreats to space systems and ensure the freedom of manoeuvre in space and through cyberspace, the full integration of emerging technologies is vitally important. The aforementioned use of quantum technologies in military applications can

strengthen cybersecurity standards and transform current platforms secured by design. For example, quantum sensors can be used for PNT instead of the existing GPS technology, which is vulnerable to jamming and spoofing techniques. Quantum PNT devices can function as a backup or replace navigation systems in case of GPS failures or attacks.

Quantum communication technologies could be employed to counter jamming and spoofing as this new technology is impervious to traditional methods of electronic warfare. AI and ML will also play a key role in vulnerability and threat detection performing much the same work in this domain as in all other domains relying on cyberspace for C2.

Blockchain platforms can also support space systems and suggest technological solutions against cyberthreats. Applying the blockchain theory in the space industry can provide decentralized and secure techniques for tracking, processing (and manipulating where possible) space resources (such as orbits, satellites, debris, asteroids, and other space objects) as space digital tokens.'[18]

These are but a few examples of how current cyberspace technologies and EDTs can benefit the space domain. However, as the cyberspace domain transcends all warfighting domains; FoM in cyberspace takes a central role in organizing and synchronizing multi-domain operations, as we will see in the next chapter.

1. A. Irei, 'What is cyber hygiene and why is it important?', TechTarget, https://www.techtarget.com/searchsecurity/definition/cyber-hygiene (accessed 19 July 2022).
2. N. Li, et al., 'Early validation of cyber–physical space systems via multi-concerns integration', Journal of Systems and Software, Volume 170, 2020, https://www.sciencedirect.com/science/article/abs/pii/S0164121220301692 (accessed 19 July 2022).
3. B. Schneier, 'Artificial Intelligence and the Attack/Defese Balance', Schneier on Security, March/April 2018, https://www.schneier.com/essays/archives/2018/03/artificial_intellige.html (accessed 19 July 2022).
4. V. Anastopoulos, D. Giovannelli, 'Automated/Autonomous Incident Response', NATO CCDCOE, 2022, https://ccdcoe.org/library/publications/automated-autonomous-incident-response/ (accessed 19 July 2022).
5. D. Fraze, 'Cyber Grand Challenge (CGC)', Defence Advanced Research Projects Agency (DARPA), https://www.darpa.mil/program/cyber-grand-challenge (accessed 19 July 2022).
6. D. Warburton, '2022 Application Protection Report: DDoS Attack Trends', F5 Labs, 16 March 2022, https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends (accessed 19 July 2022).
7. Perimeter defence seeks to prevent the introduction of malware from entering the network based on a series of technologies such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), or hybrid intrusion detection and prevention systems (IDPS).
8. Statista Research Department, 'Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030', 2022, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/#:~:text=Number%20of%20IoT%20connected%20devices%20worldwide%202019%2D2030&text=The%20number%20of%20Internet%20of,around%205%20billion%20consumer%20devices (accessed 19 July 2022).
9. CloudFlare, 'What is the Mirai Botnet?', https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/ (accessed 19 July 2022).
10. M. Amerongen, 'Quantum Technologies in defence & security', NATO REVIEW, 3 June 2021, https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html (accessed 19 July 2022).
11. D. Puyvelde, A. Brantly, Cybersecurity; Politics, Governance and Conflict in Cyberspace, Polity Press, 2019.
12. A. McAfee & E. Brynjolfsson, 'Big Data: The Management Revolution', Harvard Business Review, https://hbr.org/2012/10/big-data-the-management-revolution (accessed 26 July 2022).
13. M. Krelina, 'Quantum Technology for military applications', EJP Quantum Technology, 2021, https://epjquantumtechnology.springeropen.com/track/pdf/10.1140/epjqt/s40507-021-00113-y.pdf (accessed 19 July 2022).
14. Ibid.
15. China launched in 2016 the world's first quantum science satellite 'Micius' to provide intercontinental ground-to-satellite and satellite-to-ground ultra-secure quantum communication.
16. NIST, 'NIST Announces First Four Quantum-Resistant Cryptographic Algorithms', 5 July 2022, https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms (accessed 19 July 2022).
17. N. Hampton, Computerworld, 'Understanding the blockchain hype: Why much of it is nothing more than snake oil and spin', https://www2.computerworld.com.au/article/606253/understanding-blockchain-hype-why-much-it-nothing-more-than-snake-oil-spin/ (accessed 26 October 2022).
18. M. Torky, T. Gaber, and A. Hassanien, 'Blockchain in Space Industry: Challenges and Solutions', February 2020, https://www.researchgate.net/publication/339616244_Blockchain_in_Space_Industry_Challenges_and_Solutions (accessed 19 July 2022).

CHAPTER 6

Cyberspace Facet of Multi-Domain Operations (MDO)

6.1 Principles of MDO

NATO's digital transformation is essential to ensure that the Alliance continues to have the ability to achieve its military objectives and support its political aims. Modern security challenges shape an increasingly complex battlespace with blurred boundaries in cyberspace and information space which adversaries can leverage as attack vectors to affect all domains and levels of command. Today's military operations and conflicts reside not only in the physical dimension, but seek to create effects in the virtual and cognitive environment as well.

In the age of systemic global competition, NATO faces multifaceted threats and new dilemmas generated by assertive state and non-state actors, pushing modern warfighting beyond the traditional domains. In the Information Age,[1] NATO has realized that knowledge plays a more critical role than strength in achieving superiority in modern warfare. To meet the challenges and embrace the opportunities of the Information Age, NATO must adapt its military instruments of power from the previous 'Joint Operations' approach to a new 'Multi-Domain Operations (MDO)' force that can compete across all domains and environments.[2]

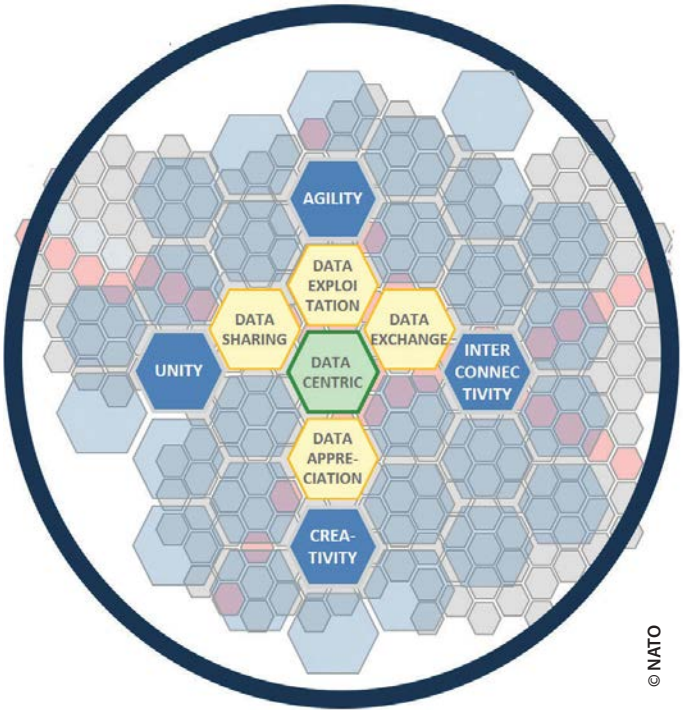


Figure 3: Overarching MDO Principles.

Based on the current agreed NATO ACT working definition, MDO is 'the orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to deliver converging effects at the speed of relevance.'[3]

'Digital Transformation of the Alliance is critical as the foundation for MDO.'[4] Establishing technological advantage against adversaries is essential if NATO wants to leverage the complexity and scale of all-source data available. NATO needs to become a data-centric organization capable of creating timely situational understanding in all five warfighting domains to achieve its three core tasks successfully in the future.

The speed and scale of modern operations require a shift from traditional thinking toward new conceptual approaches regarding the military's methods of achieving objectives. One of the prerequisites for delivering MDO is a more secure cyberspace environment, which transcends all other domains. Freedom of manoeuvre in cyberspace is vital to ensure resilience and to support the Alliance's transformation towards MDO.

Cyberspace is an enabler and enhancer of MDO. The utilization of capabilities throughout this domain provides secure communications, advanced situational awareness, and quick decision-making processes to commanders responsible for executing activities across all domains.

There are four overarching MDO principles, which apply to the activities across all domains:

Unity – Interconnectivity – Creativity – Agility.[5]

Effective MDO relies on strong collaboration, transparency and trust between military and non-military entities. Unity is difficult to achieve, but if successfully implemented through cyberspace to achieve unity across all domains, it will provide economy of effort, harmonized planning and synchronized execution.

Digital Interconnectivity is fundamental to information and decision advantage. Working on different platforms with different standardized protocols could cause interoperability issues among the various force elements undermining the mission's success.

Creativity is essential in cyberspace due to its increasingly complex and unexpected nature. The contested and shifting terrain of cyberspace offers adversaries boundless opportunities to cause surprise and create multiple dilemmas for the Alliance in the hope of affecting its operations. Creativity allows different and out-of-the-box approaches to complex challenges, simplifying, clarifying and rationalizing the problem to enable detailed planning and practical orders.

Agility is needed in modern military operations to exploit data at speed and scale across all domains and produce collective results greater than the sum of their individual parts. Especially today, as many NATO nations are establishing their own Cyber Commands and developing unique cyberspace capabilities (both defensive and offensive), it is important to accelerate the integration process of all nationally owned cyber effects.

Data centricity is a key enabler of MDO that will only be achievable in and through cyberspace. It is clearly depicted in figure 3 as the linchpin that must exist to

enable all four principles required of MDO. The Alliance needs to adapt the new data-centric mindset at the speed of relevance to build a relative advantage in shaping, contesting and fighting. Following this approach, NATO will manage to decisively influence its adversaries and defend the Euro-Atlantic area across all five operational domains.

6.2 Becoming Data-centric

In 2006, British mathematician Clive Humby coined his famous phrase 'Data is the new oil.'[6] Since then, incalculable data has been produced daily from a myriad of sensors, platforms and devices. The enormous amounts of data that is collected and available in daily operations has to be filtered, evaluated and processed to become valuable insight. As Michael Palmer explained further, like crude oil, data is 'valuable, but if unrefined it cannot really be used [...] so must data be broken down, [and] analysed for it to have value.'[7]

NATO's digital transformation, which has already begun and will culminate in MDO, is based on the realization that data is strategically vital for any organization that wants to manoeuvre securely and successfully in a data-driven world. Data is embedded in every decision, interaction, and process inside OODA loops and, therefore, has the potential to enhance nearly every military activity.[8]

In order to ensure the successful implementation of MDO, NATO needs to accelerate its efforts to support and build a data-driven ecosystem without limitations and obstacles in data processing facilities, data sharing capabilities and data exchange rates. However, cyberthreats have become more frequent, sophisticated, destructive, and coercive, undermining the security of the Alliance. Therefore, the cybersecurity and defence principles introduced in earlier chapters must be fully integrated from the onset.

According to ACT's 'Initial Alliance Concept for MDO', there are four supporting data principles that contribute to MDO's success and enhance NATO's resilience and robustness in cyberspace:[9]

- Data sharing;
- Data exchange;
- Data appreciation;
- Data exploitation.

Data sharing is crucial to enhance trust, understanding, and resilience among nations. A genuinely successful data-sharing platform facilitates collaboration and increases the speed and scale of military operations.

Data exchange consists of those pathways and gateways that link nodes to enable data sharing. Bringing together various data sources within the Alliance and other international organizations, industry and academia, the generated value becomes much greater than the sum of its parts.

Data appreciation encompasses the mindset of facilitating data supplementation and pooling to create more valuable insights and build unique data products for all allied partners.

Data exploitation directly affects the speed of decision-making as any latency between the moment a new data entry is generated and the time that data becomes available to the controller may underpin the planning and execution of MDO.

Following the above four data principles, the Alliance can extract meaningful insights from vast amounts of data across all domains quickly, efficiently and effectively. After all, NATO shall serve as the ultimate, secure, and protected platform for its 30 member nations to consult, share information, exchange best practices, and coordinate multi-domain activities.

6.3 The Multi-Domain Command and Control Advantage

As the battlespace is widening and SACEUR's Area of Responsibility is expanding to include the geographically unbound domains of space and cyberspace, together with the pervasive information environment, a new multi-domain culture needs to

be developed that will connect and integrate sensors from all military services into a single network.

Cyberspace-enabled Command and Control (C2) capabilities are generally constrained within single nations and limited by cross-border gateways. A more agile cross-domain approach is required to exploit command authorities and permissions across all domains. The existing stove-piped, domain-specific C2 architecture is insufficient, already challenged and will need to be addressed through Multi-Domain C2 (MDC2).

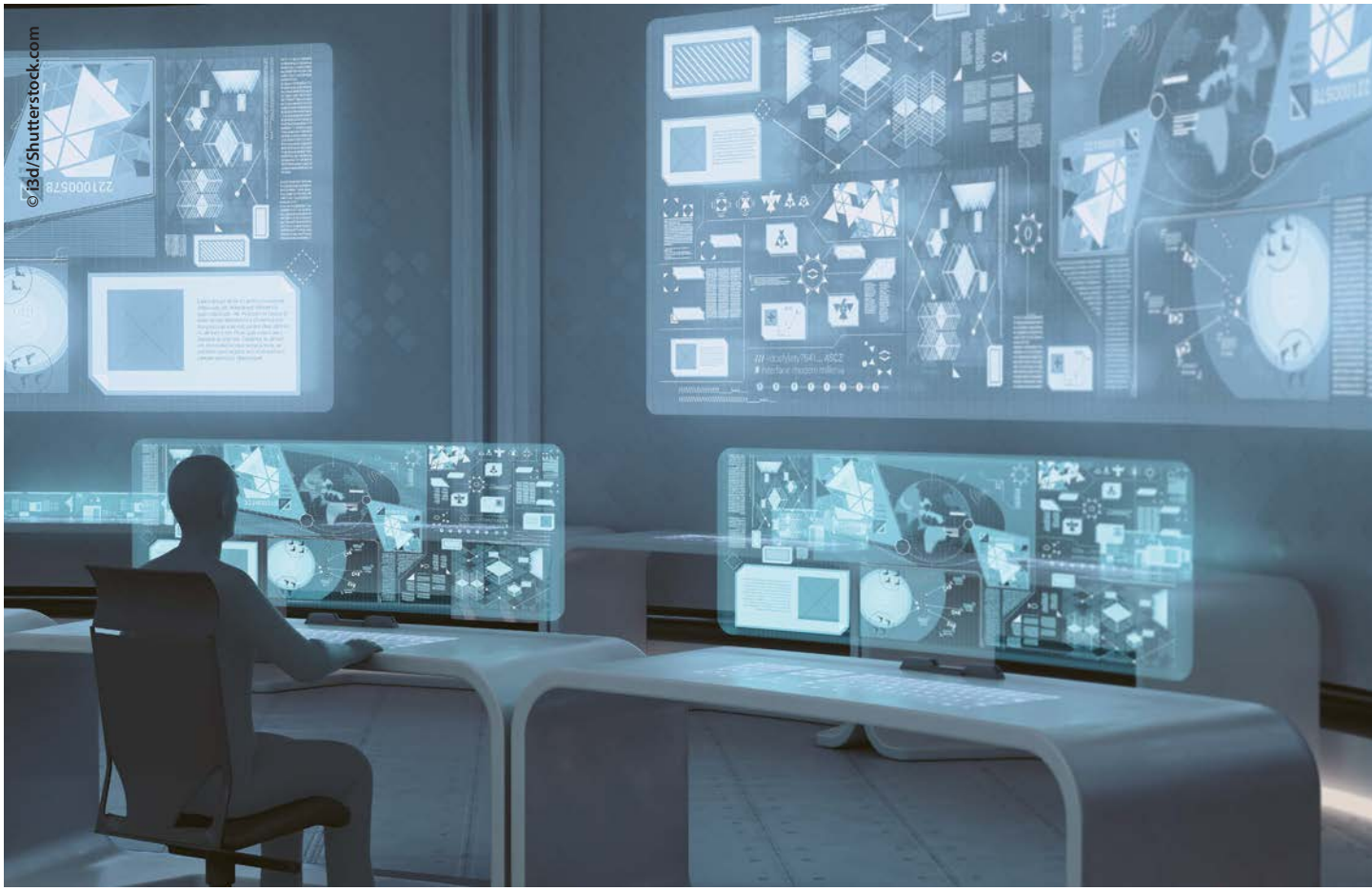
Modern operating environments and future conflicts demand decisions be made within hours and minutes compared to the previous multi-day processes. Exploiting all cross-domain options by accessing the full range of capabilities and sensors will require highly connected and decentralized OODA loops in the form of decision-making processes and platforms.

The future cloud-like combat environment will be based entirely on EDTs to increase the speed and accuracy of data analysis and accelerate the operational commander's ability to understand and act. Cloud services and infrastructure can almost instantly share and transmit data across multiple communications networks, from both the physical and non-physical domains.

Especially with the arrival of 5G, new classes of decentralized apps and protocols on the Internet are expected. The convenience of the current and emerging digital ecosystems is expected to provide more flexibility and ownership to individuals than to governments, companies, and organizations, and will empower them with self-owned identity and restore control over their data.[10] Distributed computing technologies and tools such as blockchains will lead to an increased, pluralistic, and diverse participation in the decision-making process, engaging not only the strategic and operational command levels but also the mission commanders at the tactical level with valuable and relevant experiences from diverse backgrounds and fields.[11] In modern, large and complex processes, such as military operations, where information is spread amongst various actors and each one holds only a limited part of it, a distributed decision-making model would greatly benefit the system's performance in regards to information sharing and coordination.[12]

The creation of an OODA loop in the form of MDC2 will enable commanders to understand the battlespace rapidly, direct forces faster than the enemy, and deliver synchronized combat and coherent effects.[13] Achieving timely 'information superiority' in every stage of conflict (planning, deployment, and engagement) will allow future commanders to gain the decision advantage, project power effectively, and shape the battlespace.

1. E. Lawson, 'Warfare in the Information Age', RUSI Journal, Vol. 161, Issue 5, 30 November 2016, https://rusi.org/explore-our-research/publications/rusi-journal/warfare-information-age (accessed 19 July 2022).
2. NATO ACT, 'Initial Alliance Concept for Multi-Domain Operations' (Executive Summary), July 2022.
3. Ibid.
4. NATO ACT, 'Multi-Domains Operations Conference – What We Are Learning', 8 April 2022, https://www.act.nato.int/articles/multi-domains-operations-lessons-learned (accessed 19 July 2022).
5. Ibid. 2.
6. M. Watts, futurescot.com, 'Why data is the new oil', https://futurescot.com/why-data-is-the-new-oil/, (accessed 25 October 2022).
7. M. Palmer, 'Data is the New Oil', 3 November 2006, https://ana.blogs.com/maestros/2006/11/data_is_the_new.html (accessed 19 July 2022).
8. McKinsey, 'The data-driven enterprise of 2025, QuantumBlack, AI by McKinsey, https://www.mckinsey.com/business-functions/quantumblack/our-insights/the-data-driven-enterprise-of-2025 (accessed 19 July 2022).
9. Ibid 2.
10. A. Jones, 'What is Web5?', TBD, 1 July 2022, https://developer.tbd.website/blog/what-is-web5/ (accessed 19 July 2022).
11. Blockchains are computer files used for storing data, which are publicly distributed and encoded across many computers. As a result, no one (person or entity) has control over the content of the file making it extremely difficult to edit it.
12. M. Lujak et al., 'Scalable Distributed Decision-Making and Coordination in Large and Complex Systems: Methods, Techniques, and Models', 31 July 2020, https://www.hindawi.com/journals/complexity/2020/1425909/ (accessed 19 July 2022).
13. CRS Report, 'Joint All-Domain Command and Control (JADC2)', updated 21 January 2022. https://sgp.fas.org/crs/natsec/IF11493.pdf (accessed 19 July 2022).



CHAPTER 7

Conclusion

The emergence of cyberspace in recent decades has already transformed humankind, including how it competes, how it fights wars, and even how it maintains the peace. The pace of technological advances is only accelerating and even greater changes are expected in the years ahead as we grapple with EDTs and develop new and yet-to-be-imagined ways of leveraging them in all human endeavours. If we are not already starting to think about how to evolve our FoM abilities in cyberspace and how to integrate EDTs quickly, we are already one step behind and will eventually lose the technological advantage.

By its very nature, the cyberspace domain permeates and transcends all other warfighting domains. Regardless of our respective ranks or roles in the air force, army or navy, when one of us picks up our cell phone, sits down at a computer, or operates a sensor or weapon platform, we instantly become frontline combatants in the cyberspace domain.

This was not a deliberate choice. We joined to be pilots, air weapons controllers, naval officers, infantrymen, engineers, and a host of other occupations that piqued our interest. Yet, we find ourselves simultaneously in the 'cyberspace trenches' in what can become, at any moment, a virtual or literal shooting war. This could have immediate repercussions, not only in our small portion of cyberspace, but also in our respective warfighting domains. Moreover, the risks of

catastrophic failure will continue to increase significantly, as our reliance on cyberspace systems also increases our drive to accelerate our OODA loops unless we build in resiliency and response mechanisms.

Dedicated cyberspace operations capabilities and units will have a significant role to play as well. However, we must consider them as we think of capabilities such as artillery and area air defence systems. In other words, defence in-depth capabilities that lend support and strengthen the frontline are unable to win the battle all on their own, but are essential to any victory.

Gaining a general appreciation of what FoM in cyberspace is, becomes necessary for most military personnel who rely on technology to accomplish their assigned tasks. This may not be what any of us signed up for, but in this highly technological and increasingly connected world, it is the reality that we must embrace. Otherwise, we run the risk of becoming the first casualty in a fight that may begin for any one of us in cyberspace, but will quickly spill into our respective traditional warfighting domains, with equally devastating results, not only for ourselves but also for our peers and units as a whole.

Future warfighting will include cyberspace in all domains and for everyone involved; it is unavoidable but is not yet acknowledged by all involved. Whether and how quickly NATO embraces new concepts and integrates the newest technologies will be the difference between keeping that advantage over our adversaries or not.

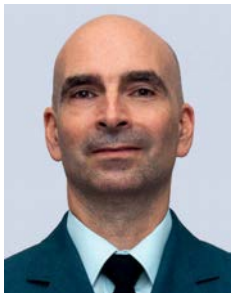
ANNEX A

Acronyms and Abbreviations

3DES	Triple DES
AI	Artificial Intelligence
APT	Advanced Persistent Threat
C2	Command and Control
CIA Triad	Confidentiality, Integrity, and Availability Triad
CNI	Critical National Infrastructure
CO	Cyber Operations
DARPA	Defence Advanced Research Projects Agency
DCO	Defensive Cyberspace Operations
DDoS	Distributed Denial of Service
DES	Data Encryption System
EDTs	Emerging and Disruptive Technologies
FoM	Freedom of Manoeuvre
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IoT	Internet of Things
IPS	Intrusion Prevention System
MDC2	Multi-Domain Command and Control
MDO	Multi-Domain Operations
ML	Machine Learning
NFT	Non-fungible token
NIST	US National Institute of Standards and Technology
NOTAMs	Notice to Air Missions
NSA	United States National Security Agency
OODA loop	Observe/Orient/Decide/Act loop
QC	Quantum Computing
PNT	Position, Navigation, and Timing
SA	Situational Awareness
SATA	Serial Advanced Technology Attachment
SDRs	Software Defined Radios
SIEM	Security Information and Event Management
SME	Subject Matter Expert
TTPs	Tactics, Techniques, and Procedures
ZB	Zettabyte

ANNEX B

About the Authors



Lieutenant-Colonel Eric Jodoin

earned a Master of Science in Information Security Engineering (MSISE) from the SANS Technology Institute in 2015 and holds the Certified Information Systems Security Professional (CISSP) certification since 2009. He has accumulated over a dozen years of experience in the planning and conduct of full-spectrum cyberspace operations.

He spent the first decade of his military career in the Royal Canadian Navy (RCN) as a Maritime surface and subsurface (MARS) Officer, honing his warfighting and operational planning skills before transferring to the Royal Canadian Air Force (RCAF) as a Communication & Electronics (CELE) Officer where he transmuted his love of hacking into a vocation as an Information System Security Officer, Information Assurance specialist, cybersecurity professional, and finally a cyberspace SME.

His experience includes a tour as Director of Operations at the Canadian Forces Network Operations Centre (CFNOC), where he contended with a mix of insider threats, crimeware, and advanced persistent threats (APTs). He was the Chief Instructor on the Canadian Forces Cyber Operations Staff Officer (CFCOSO) Course in 2012 and guest lecturer on various cyberspace operations courses, and public events such as BSIDES Ottawa 2014 and SANS Network Security 2014 in Las Vegas. He was a cyberspace operations planner for Canada in support of multinational operations including Operation Inherent Resolve, and lead of the Cyber Component Coordination Element (CCCE) embedded within the Canadian Joint Operations Command (CJOC).

Major (ret.) Fotios Kanellos

graduated from the Hellenic Air Force (HAF) Academy in 2003 as an Electrical Engineer specializing in Telecommunications and Computer Science. He holds three Master's degrees, one in Technical-Economic Systems from the National Technical University of Athens (NTUA), one in Environmental Sciences from the University of Patras and another in European and International Studies from the National and Kapodistrian University of Athens.

He served as an inspection engineer for T-2 C/E aircraft, system engineer for the T-6A Flight Simulator, and as the Head of IT Department at the Hellenic Air Training Command (HATC) in Kalamata. During his last two years in the aforementioned Air Base he served in the Quality Assurance Department reaching the position of the department head.

His previous appointment was as senior officer, and later, the head of Informatics Department at the HAF Support Command (HAFSC) leading and managing various IT and Cybersecurity projects over more than a dozen subordinate units and combat wings. He has also been an instructor at the Hellenic Air Force NCO Academy providing cybersecurity and software programming courses.

Finally, he has participated in national and multinational exercises supporting the Cyber Opposing Forces (OPFOR) by scripting and executing cyber injects for the training audience.

During his assignment as a Cyberspace SME at JAPCC, he researched and contributed to several articles promoting the development and integration of Cyberspace in NATO Joint Air Power.

Joint Air Power Competence Centre

von-Seydlitz-Kaserne
Römerstraße 140 | 47546 Kalkar (Germany) | www.japcc.org