Published by CCDCOE

Cyber Commanders' Handbook 2



CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

CYBER COMMANDERS' HANDBOOK 2

Copyright © 2025 by NATO Cooperative Cyber Defence Centre of Excellence.
All rights reserved.

ISBN (print): 978-9916-9789-6-2
ISBN (pdf): 978-9916-9789-7-9

COPYRIGHT AND REPRINT PERMISSIONS

No part of this publication may be reprinted, reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the NATO Cooperative Cyber Defence Centre of Excellence (publications@ccdcoe.org).

This restriction does not apply to making digital or hard copies of this publication for internal use within NATO, CCDCOE member nations or for personal or educational use when for non-profit or non-commercial purposes, providing that copies bear this notice and a full citation on the first page as follows:

Cyber Commanders' Handbook 2
F. Hickey, B. Magurno, S. Pastor, N. Rodrigues, D. Štrucl (Eds.)
2025 © NATO CCDCOE Publications

NATO CCDCOE Publications
Filtri tee 5, 10132 Tallinn, Estonia
Phone: +372 717 6800
Fax: +372 717 6308
E-mail: publications@ccdcoe.org
Web: www.ccdcoe.org
Layout: Jco Design Factory

LEGAL NOTICE: This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE). It does not necessarily reflect the policy or the opinion of the NATO CCDCOE, NATO, or any agency or government. The NATO CCDCOE may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited knowledge hub that takes a distinctive interdisciplinary approach to the most relevant issues in cyberspace. At its core, the NATO CCDCOE is staffed by a diverse array of international experts from military, governmental, academic, and industrial backgrounds, representing 39 like-minded nations from across the globe.

The NATO CCDCOE is a leading authority on cyber defence related matters, offering invaluable expertise in strategic, legal, operational, and technical realms. It serves as a beacon of innovative thought in all facets of cyber defence, providing a comprehensive perspective on the field. The NATO CCDCOE encourages and supports the process of mainstreaming cyber defence into NATO and national governance and capability within its closely connected focus areas of technology, strategy, operations, and law.

The *Tallinn Manual*, developed at the initiative of the NATO CCDCOE, serves as the most comprehensive guide for legal experts and policy advisers on the application of international law to cyberspace operations involving states and non-state entities. The NATO CCDCOE also co-produces the Cyber Law Toolkit, an interactive tool for all those working at or interested in the intersection of cyberspace operations and public international law.

Since 2010, the NATO CCDCOE has organised the Locked Shields exercise, recognised as the world's largest and most complex live fire technical cyber resilience exercise. Every year, cybersecurity professionals participate in Locked Shields to hone their abilities to safeguard national IT systems and critical infrastructure amid real time cyberattacks. The exercise is designed around realistic scenarios, cutting edge technologies, and a comprehensive cyber incident simulation, encompassing strategic decision making, legal considerations, and communication strategies. In addition, the NATO CCDCOE organises the annual Crossed Swords exercise. Crossed Swords set against the background of the fictional world of Berylia, is a full spectrum cyberspace operations exercise which brings together cyber command headquarters and technical operators to train in the planning and execution of cyberspace operations in a wider military context.

The NATO CCDCOE hosts the International Conference on Cyber Conflict, known as CyCon. This unique event has taken place every May in Tallinn since 2009. CyCon brings together prominent experts and decision makers from the global cyber defence community, attracting over 600 attendees from governments, industry, and academia.

The NATO CCDCOE is responsible for identifying and coordinating education and training solutions in cyber defence operations for all NATO bodies across the Alliance and member nations of the NATO CCDCOE.

DOCUMENT INFORMATION

Project lead:

- Comdt Frank Hickey , Operations Branch, NATO CCDCOE

Project team:

- Maj Battista Magurno, Operations Branch, NATO CCDCOE
- Lt. Col Nuno Rodrigues, Strategy Branch, NATO CCDCOE
- Lt. Col Erdi Donmez, Strategy Branch, NATO CCDCOE
- Lt. Col Nick Wobma, Law Branch, NATO CCDCOE
- Kerim Kalipcioglu, Technology Branch, NATO CCDCOE

Contributors and editors:

- Capt Vasco Marques Prates, Strategy Branch, NATO CCDCOE; Portuguese Naval Staff
- Lt. Col Sergio Pastor, Operations Branch, NATO CCDCOE
- Lt. Col Boyan Devedzhiev, Operations Branch, NATO CCDCOE
- James Austin, Operations Branch, NATO CCDCOE
- Maj Marco Schneeberger, Operations Branch, NATO CCDCOE
- Dr Sigurður Emil Pálsson, Operations Branch, NATO CCDCOE
- Lt. Col Damjan Štrucl, Strategy Branch, NATO CCDCOE
- Yongkuk Cho, Strategy Branch, NATO CCDCOE
- Maj Andrii Davydiuk, Plans and Coordination Branch, NATO CCDCOE
- Bjoern Gunnvall Ekstorm, Swedish Armed Forces
- Luca Schmid, Swiss Armed Forces
- Pierre Kilchenmann, Swiss Armed Forces
- Lt. Comdr Luis Velho, Cyber Defence Operations Command Portugal
- Jakub Fucik, Czech Armed Forces
- Sander van Dorst, Cyber Warfare and Training Centre, Netherlands Ministry of Defence
- Lt. Col Fabio Biondi, Italian Cyber Command
- Lt. Col Massimiliano Signoretti, Italian Cyber Command
- Maj Pasquale Iorillo, Italian General Defence Staff
- Arnold Ten Dam, NATO Cyberspace Operations Centre (CyOC)
- Lt. Florian Khanh, French Defence Ministry
- Alan Sewell, Swedish Defence University
- Lt. Col Lars Koreman, DtA Cyberspace Operations Centre, SHAPE
- Sandra Laur, Strategy Branch, NATO CCDCOE; Kings College London
- Col Josef Schroefl, European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE)s

- Brig. Gen Oleksandr Potii, State Service of Special Communications and Information Protection of Ukraine
- Maj John Dall, Strategy Branch NATO CCDCOE

Version 2.0

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE). The NATO CCDCOE does not speak on behalf of NATO, and the research done in the centre does not necessarily reflect the policy or the opinion of NATO, NATO CCDCOE, member nations of CCDCOE, or any agency or government.

Authorised by: Dr Mart Noorma
Director, NATO CCDCOE
Release date: May 2025

CONTENTS

FOREWORD 9

EXECUTIVE SUMMARY 10

1. INTRODUCTION 12

1.1 Scope 12
1.2 Development Process 12
1.3 Target Audience 12
1.4 Structure 12
1.5 Application 13
1.6 Definitions and Descriptions 13

2. STRATEGIC VIEW, CYBER DEFENCE CONCEPTS, AND THE THREAT LANDSCAPE 14

2.1 Strategic Environment 14
2.2 Cyber Defence Concepts 16
2.3 Threat Landscape 26
2.4 Trends Shaping the Threat Landscape 30
2.5 National Cyberspace Actors 31

3. CYBERSPACE AS A DOMAIN OF OPERATIONS 33

3.1 The Layers of Cyberspace 35
3.2 Cyberspace Zones 37
3.3 Cyberspace and Multi-Domain Operations (MDO) 39
3.4 Cyberspace and Electromagnetic Activities (CEMA) 40
3.5 Cyberspace Areas of Operation 42
3.6 Terrain Analysis in Cyberspace 43
3.7 Using Terrain Analysis to Understand the Digital Battlespace 45
3.8 Cyberspace Terrain Analysis Model 45
3.9 Cyber Common Operational Picture (Cyber COP) 47
3.10 Cyberspace and the Total Defence Approach 48
3.11 Characteristics of Cyberspace Operations 49
3.12 Cyberspace Opportunities and Challenges 50
3.13 Attribution 52
3.14 Reference Cyber Command Structure 53
3.15 Cyberspace Manoeuvre Elements 55
3.16 Creating the Cyber Battlespace 57

4. CYBERSPACE OPERATIONS 59

4.1 Characteristics of Effective Cyberspace Operations 60
4.2 Communication and Information Systems Operations (CISOPS) 61

4.3 Defensive Cyberspace Operations (DCO) 64
4.4 Cyberspace Intelligence, Surveillance, and Reconnaissance Operations (CyISR) 66
4.5 Offensive Cyberspace Operations (OCO) 69
4.6 Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) 70
4.7 Phases of a Cyberspace Operation 71
4.8 Legal Considerations Related to Different Operations 72

5. CYBERSPACE OPERATIONS PLANNING 76
5.1 Political, Strategic, and Operational Prerequisites 76
5.2 Cyber Considerations and Operational Planning 77
5.3 Planning Considerations 81
5.4 Assessment 86

6. CYBERSPACE TOPICS 88
6.1 Civil-Military Cooperation (CIMIC) 88
6.2 Quantum Technology 91
6.3 The Cyber-Hybrid Intersection 94
6.4 Threat Discovery (Threat Hunt/Emulation and Purple Teaming) 96
6.5 Cyberspace Resilience 99
6.6 How AI is Changing Cyberspace Operations 102
6.7 Experience and Lessons from Ukraine 105

CONCLUSION 109

ANNEXES 110
Annex A Definitions and Acronyms 110
Annex B Cyber Prioritised Asset List (CPAL) 117
Annex C Functional Areas and Special Advisors 118
Annex D References 122

FOREWORD

In our increasingly interconnected world, the IT systems and critical infrastructure that underpin our societies have become frequent targets for cyber exploitation. The systems that sustain our daily lives are under constant threat, and the potential consequences are more severe than ever. Cyberspace represents both an opportunity and a risk, providing adversaries with new avenues to disrupt national security and economic prosperity. This complexity means we must use our limited resources efficiently to respond swiftly and effectively.

Recent conflicts have highlighted cyberspace as a critical operational domain. We are increasingly seeing cyber capabilities used in geopolitical competition, hybrid warfare, and conflict. Cyberspace operations are no longer limited to espionage or disruption – they are now employed as weapons at every level to shape battlespaces. The ability to operate effectively in cyberspace is becoming a decisive factor in modern conflict, making preparedness and agility more essential than ever.

The *Cyber Commanders' Handbook 2* is an essential resource for anyone working in the cyberspace domain. It serves as a reference for those working in or alongside cyber commands, as well as for individuals seeking to deepen their understanding of cyberspace operations. By compiling ideas and concepts from an international perspective, the handbook offers guidance on building, leading, and operating within this domain.

Cyberspace is a dual use technology, predominantly owned and operated by private industry, which raises a unique question: How do we integrate civilian expertise and infrastructure to assure missions? Civil-military collaboration will be critical as we prepare for emerging threats and future technologies that will reshape the operational landscape. This requires developing robust partnerships and fostering cyber awareness in everyday planning, activities, and operations.

The *Cyber Commanders' Handbook* is an international reference for cyberspace. I commend it to you. Cyberspace is a domain of both opportunity and challenge, and those who adapt to the ever changing environment will define its future.

Ana L Duncan, AM, CSC
Major General
Commander Cyber Command
December 2024
Australian Defence Force

EXECUTIVE SUMMARY

This Cyber Commanders' Handbook 2 provides an international perspective and framework to understand the cyberspace environment and concepts related to the planning, coordination, execution, and assessment of cyberspace operations. It outlines the roles, responsibilities, and core activities of a cyber command. It is a collaborative product of the NATO CCDCOE and national cyber defence experts.

Cyberspace enables continuous access to information and services, creating the opportunity for state and non-state actors to use cyberspace to assert influence in the political, military, economic, and social spheres. The complexity of cyberspace is compounded by many factors, such as the cyber skills gap, emerging technology, and supply chain interdependencies. To operate effectively and mitigate risks in cyberspace, a key requirement will be to build trust between key stakeholders and foster cross disciplinary collaboration between siloed technical and operational communities.

Recent conflicts have shown how cyberspace can be used and exploited. Lessons from these operations demonstrate their strengths and limitations. These lessons will drive innovation, and cyberspace operations have the potential to become more decisive in future conflicts. The Cyber Commanders' Handbook 2 gives an overview of the general division of responsibilities at the national level and provides a reference structure for a cyber command. Effective cyberspace operations require collaboration across society, leveraging partnerships with industry and academia. Such cooperation is essential for innovation, capacity building, and addressing the complexity of the cyberspace domain. Furthermore, as cyberspace is not owned nor the responsibility of any one organisation, collaboration across the whole of society and the whole system will become even more critical than ever. The whole-of-society approach emphasises collective responsibility for cybersecurity by engaging governments, military, businesses, civil society, and individuals to create a culture of awareness, collaboration, and shared action. This approach, once established, allows the key stakeholders to understand each other's roles and responsibilities in the transition from peace to crises and conflict.

As there is no unified cyberspace terminology and lexicon, organisations have different understandings of cyberspace, which adds to the complexity of operating in cyberspace and designing adequate response options. When a common understanding of cyberspace is achieved, it can be viewed as both an environment and a domain of operations. This enables efficiency and unity of effort in cybersecurity, cyber defence, and cyberspace operations.

Cyberspace is a domain of operations where actions and effects can be delivered, supporting mission assurance. Cyber actions occur in one or more of the seven layers of cyberspace. Offensive and defensive actions or capabilities are temporary, and no advantage is permanent. Moreover, no one nation can assert sovereignty over cyberspace. Instead, there is sovereign equality among nations. Sovereignty remains over physical assets, individuals, and territory. These features create several challenges, such as the complexity of attribution or conflict between time consuming preparations and a quickly changing threat landscape. As cyberspace is just a different domain of operations, the ideas and concepts already well established in other operational domains apply to cyberspace. While it is challenging due to the virtual nature of cyberspace, this includes observing, viewing, and describing cyberspace in terms of zones, terrain, areas of operation, and responsibility.

As there is no one approach to building a cyber command. The Cyber Commanders' Handbook 2 provides a reference architecture that allows cyberspace operations' core activities to be efficiently coordinated with unity of effort and unity of purpose. It focuses on the four types of cyberspace operations, their differences, and the key skills and functions needed to achieve them. While cross team support is vital and some skills and functions are common to more than one type of cyberspace operation, dedicated cyber operation teams must be developed. In addition, the cyber battlespace needs to be created, which includes the physical infrastructure, and virtual environments to conduct cyberspace operations, as well as the cyber ranges required to train and develop skills on. This ensures cyberspace forces can be prepared and postured to operate effectively with clear authorities and approval processes.

Cyberspace operations enhance a nation's cyber resilience and ability to act as a sovereign state in peacetime and achieve military advantage in crises and conflict. The handbook provides a framework for cyberspace operations. Cyberspace operations can require extensive preparation. Therefore, cyberspace must be considered as early in the planning process as possible. There are also other areas in the planning process, such as authorisation processes, timelines, targeting, and effects, that need additional consideration due to the characteristics of cyberspace.

This handbook equips cyber commanders' with the knowledge to lead cyberspace operations efficiently while addressing the unique challenges posed by cyberspace. It also seeks to enhance the awareness and understanding of a cyber commanders' staff as well as others working alongside cyber command, highlighting the need for a comprehensive, collaborative, and adaptable approach to cyberspace operations.

1. Introduction

1.1. SCOPE

This publication is an initiative of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE). It provides an independent perspective that supports the understanding of cyberspace and the assessment, planning, and execution of cyberspace operations. Companion publications are planned that will examine specific aspects of cyberspace operations in more detail.

1.2. DEVELOPMENT PROCESS

The project aimed to develop an understanding of cyberspace at the strategic and operational levels and introduce technical and legal aspects into a practical guide that can be used at a national level by those who work in, or need to understand, cyberspace operations. The *Cyber Commanders' Handbook 2* has been developed in close cooperation with subject matter experts from national cyber commands and other relevant national and NATO entities. The handbook's concept, structure, and contents were based on version 1 and developed through several workshops and written submissions. The process was designed to obtain expert insight, best practices, and real life lessons learned by the contributing nations to ensure that the handbook would be relevant and address the needs of its target audience. The final version of the handbook was coordinated with all contributors, capturing their feedback and comments.

The handbook reflects the evolving state of national commands, doctrine, and operations and the rapidly changing nature of cyberspace.

1.3. TARGET AUDIENCE

The target audience for the Cyber Commanders' Handbook 2 comprises the cyber commander and their staff, military personnel from all services, and government officials who collaborate with cyber commands or anyone who would benefit from a deeper understanding of cyberspace and cyberspace operations.

1.4. STRUCTURE

The handbook is divided into six chapters, covering concepts and ideas related to cyberspace and cyberspace operations. Chapter 1 gives an overview of the

handbook's scope, target audience, and purpose. The overall context of cyberspace operations and the threat landscape is introduced in Chapter 2. Chapter 3 describes cyberspace as a domain of operations and describes how to examine cyberspace in terms of terrain. Furthermore, this chapter introduces a reference cyber command structure and cyberspace manoeuvre elements. In Chapter 4, the handbook goes into depth regarding four types of cyberspace operations: Communication and Information Systems Operations (CISOPS); Cyberspace Intelligence, Surveillance and Reconnaissance Operations (CyISR); Defensive Cyberspace Operations (DCO); and Offensive Cyberspace Operations (OCO). In addition, chapter 4 breaks down cyberspace into operational phases as well as legal considerations. Chapter 5 covers cyber considerations for the planning process, as well as coordination, execution, and assessment. In Chapter 6, the handbook discusses various cyberspace related topics in more detail. In particular, what lessons can be drawn from Ukraine.

1.5. APPLICATION

This publication is non-authoritative and is applicable in peacetime, crisis, and conflict situations.

1.6. DEFINITIONS AND DESCRIPTIONS

To be able to discuss and/or explain aspects of cyberspace operations, descriptions and definitions must be understood unambiguously. Because no complete set of agreed definitions is available, this handbook will use the accepted definitions from organisations such as NATO, ENISA,[1] and the US Department of Defense. Wherever necessary, working definitions will be added. Readers should be aware that definitions and terminology are constantly under review, and some will likely change in the future. To maintain a common understanding, readers should refer to the most recent agreed versions.

1 ENISA – European Union Agency for Cybersecurity.

2. Strategic View, Cyber Defence Concepts, and the Threat Landscape

2.1 STRATEGIC ENVIRONMENT

Global security relies on international stability and prosperity. As society becomes more dependent on services delivered through cyberspace, new means of influence and coercion have emerged. While cyberspace provides significant benefits, its interconnected nature also introduces vulnerabilities and concerns related to security, resilience, and the global supply chain. Cyberspace is an ever changing, continuously contested environment. Nations increasingly face sophisticated threats from cyberattacks, espionage, and cyberattacks on critical infrastructure and essential services.

Due to the interconnected nature of cyberspace, cyberattacks and other incidents can have regional and global consequences. The complexity in the cyberspace environment is driven by a number of compounding factors such as the cyber skills gap, artificial intelligence, emerging technology, supply chain interdependencies and geopolitical tensions.[2] Resilience, security, and the ability to continue operations during cyber events must be built into systems and functions at the organisational and national levels. Cybersecurity and cyber defence require a whole-of-society and whole-of-system approach, where government, the military, the police, the cybersecurity industry, and legal, academic, and industrial sectors collaborate holistically. Policy makers and stakeholders must integrate cybersecurity into legislation and strategies. In addition, an environment must be developed where trust is built and cross disciplinary collaboration between siloed technical and operational communities is fostered.[3]

Cyberspace is the fifth operational domain, alongside land, sea, air, and space, as declared by NATO at the Warsaw summit in 2016 and by the EU in the European Cyber Defence Policy Framework 2018.

Adversaries often operate below the threshold of armed conflict, extending their influence without resorting to physical actions. This ‘new normal’ allows them to provoke and intimidate nations, citizens, and organisations without fear of legal or military repercussions. Western nations, with their traditionally high thresholds for responding to adversarial activities in cyberspace, are particularly vulnerable.

2 (WEF, 2025)
3 (Piret Pernik, 2025)

Adversaries exploit these dependencies and vulnerabilities to weaken democratic institutions and gain economic, diplomatic, and military advantages.

Government, military, critical infrastructure, essential services, the supply chain, and network infrastructures are vital for the smooth functioning of civil society and military operations. These networks face a broad range of threats from cyberspace actors who continuously develop tactics, techniques, and procedures (TTPs) to evade detection and overcome generic security measures. Cyberattacks are becoming more frequent and complex, with a reduced time from reconnaissance to the exploitation of vulnerabilities. These threats are global, transcending geographic boundaries, and are now inherent in modern conflicts.

Militaries and governments have become reliant on cyberspace infrastructure, which is continuously contested by state and non-state actors targeting networks, devices, and people for strategic advantage. Much of this infrastructure is not owned by governments or the military. Similarly, much of the knowledge and capability in cyberspace is with the civilian and private sectors. The dual use nature of cyberspace increases the complexity of operating in this domain.

Recent conflicts demonstrate how cyberspace can be strategically leveraged before conflict breaks out as well as during military operations and how cyberspace operations impact civilian populations throughout. In future conflicts, collaboration with public and private partners and sharing knowledge between civil and military experts will be crucial.[4] In addition, the need to continuously innovate in cyberspace is vital. The success of military operations depends on continuous access to cyberspace. Inadequate resilience, agility, and operational capabilities in the cyberspace domain, encompassing people, processes, and technology, give adversaries a significant advantage. This can pose substantial risks to generating and employing combat power for military purposes. Losing access to or freedom of manoeuvre in cyberspace during crises or conflicts will degrade operational effectiveness. As cyberspace vulnerabilities get closer to individual weapons systems, commanders' at all levels must be aware of how cyber incidents can affect the mission.

In an international contested environment, countries and entities such as NATO and the European Union (EU) aim to ensure peace, international stability, cooperative security, and collective defence. If we do not position ourselves effectively before any conflict, ensuring freedom of movement and information superiority, national sovereignty cannot be assured. Without a comprehensive understanding of cyberspace, electromagnetic warfare, signals intelligence, and space, a strong and effective cyber defence capability cannot be achieved.

4 (Landry, 2023)

Aligned with the EU/NATO joint declaration,[5] cyber defence pledge,[6] and national cyber capability development, countries have been developing cyberspace forces for several decades. Many nations have made statements on the applicability of international law in cyberspace. and established or are establishing cyber commands to conduct 'full spectrum cyberspace operations'. Previously, it was typical for countries to focus on communication and information system (CISOPS) operations, security, and defensive cyberspace operations capabilities, but now, many countries are publicly announcing the development of offensive cyber capabilities. Additionally, cyberspace and the electromagnetic spectrum are increasingly considered intrinsically linked and part of the 'information environment'.

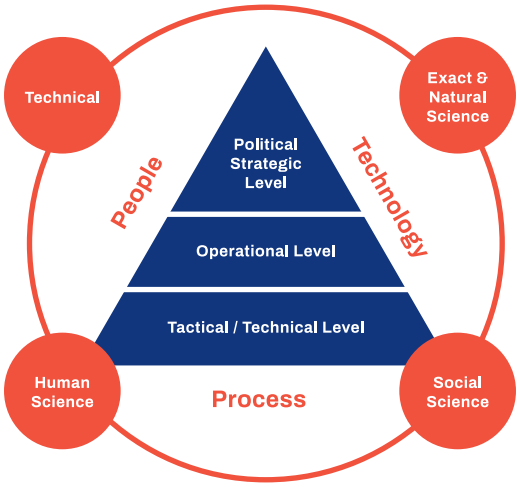
To conduct cyberspace operations, cyber commands need an appropriate organisational structure, civil and military cooperation, principles and guidelines outlining their mission, and tasks, roles, and responsibilities. These should include command and control (C2), political authorisation, military authorisation, strategic/operational guidelines, standard operating procedures (SOPs), and key technical functions that enable CIS operations (CISOPS), Defensive Cyberspace Operations (DCO), Cyberspace Intelligence Surveillance and Reconnaissance (CyISR), and Offensive Cyberspace Operations (OCO).

2.2 CYBER DEFENCE CONCEPTS

With the accelerated development of information and communication technology (ICT), the security environment has undergone significant changes, blurring the line between peace and war. This is primarily because individual components of the contemporary security environment are broadly defined, leading to challenges in understanding it both nationally and internationally. Cyberspace, as a part of the information environment, has reshaped the global security environment and prompted significant discussions at all levels. Therefore, a holistic and interdisciplinary approach is needed (Figure 2-1).

5 (EU_NATO, 2023)
6 (NATO, 2016)

FIGURE 2-1: A HOLISTIC AND INTERDISCIPLINARY APPROACH TO CYBERSECURITY/DEFENCE



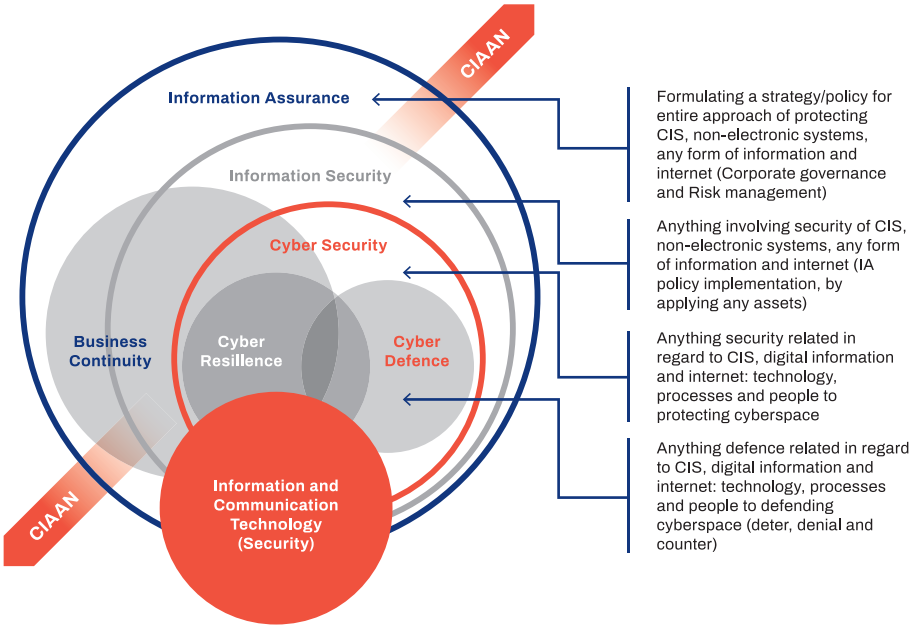
Additionally, cybersecurity and defence not only depend on understanding ICT but also require an interdisciplinary approach that enables effective coordination, cooperation, and collaboration among various stakeholders. This also results in the synergy between the civilian and military sectors.

Challenges Faced with Cybersecurity Taxonomy

Various nations and organisations, such as NATO and the European Union (EU), have agreed on several IT standards. Nevertheless, there is no internationally agreed upon cyberspace and cybersecurity taxonomy. The cyber commander must be aware that different countries, organisations and groups view cyberspace differently depending on their understanding of the definitions. Therefore, the effective implementation of cyber defence will present challenges unless an adequate level of cybersecurity, information security, and information assurance taxonomy is established. Likewise, effective coordination, cooperation, collaboration, and joint response cannot be achieved when some states understand cybersecurity to be synonymous with information security and others do not.

Cyber commanders' should consider cyber related security taxonomy (Figure 2-2) to avoid misunderstanding between civilian and military stakeholders at a national and international level.

FIGURE 2-2: CYBER RELATED SECURITY TAXONOMY (ŠTRUCL, 2022), P. 7; ADAPTED FROM ISO 27000 SERIES ISO 22301, AND NIST CYBER SECURITY FRAMEWORKS)[7]



Information Environment

The information environment can be defined as: 'the interconnected functioning of CIS, individuals and organisations within the physical, virtual, and cognitive dimensions, in which cyberspace enables their global interaction and activities' (Figure 2-3).[8]

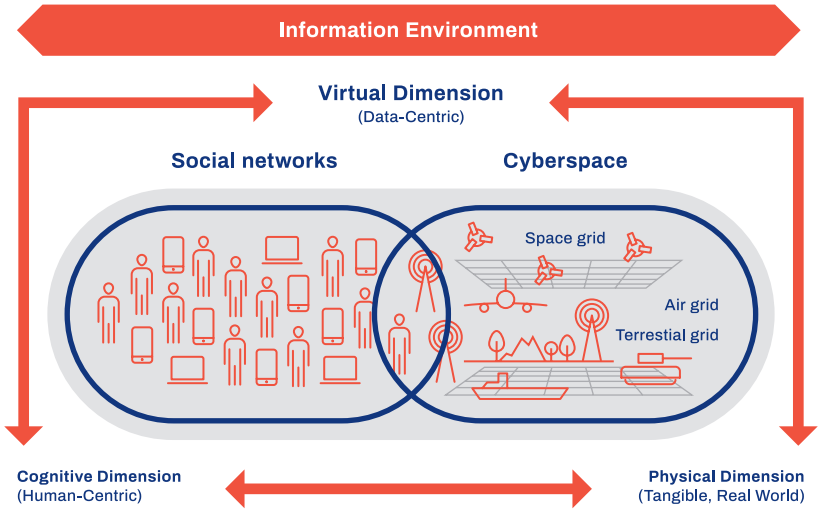
Cyberspace is a part of the information environment. Without adequate information security policy and cybersecurity policy, there is no effective cyber defence and vice versa. In doing so, it is necessary to consider all dimensions of cyberspace, to be aware of the cascading effects, and to observe the rules of international law that offer protection to the civilian population.

Therefore, cybersecurity and cyber defence must consider the entire information environment, in which cyberspace (technically) enables global interaction and activities between three interrelated dimensions: physical, virtual, and cognitive.

7 CIAAN – Confidentiality, Integrity, Availability, Authentication, Non-Repudiation
8 (Štrucl, 2022), p. 27.

The entire information environment facilitates a wide range of hybrid activities.[9] Cyberspace makes this possible while, at the same time, blurring the boundary between military and criminal activities. Hence, a comprehensive approach to cybersecurity and defence relies not only on technical measures but also on a deep understanding of the complex interplay between technology, society, and geopolitics. At the same time, a comprehensive approach enables synergy between civil and military structures.

FIGURE 2-3: INFORMATION ENVIRONMENT (PORCHE III, 2016, P. 2, JOINT PUBLICATION 3–13: INFORMATION OPERATIONS, 2014, PP. 1–2)



Cyberspace Environment

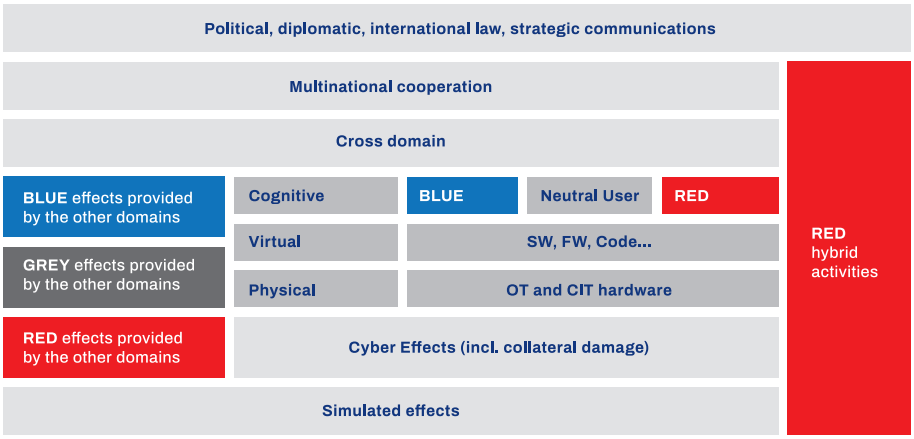
The cyberspace environment can be defined as:'The interconnected digital space where information and communication technologies facilitate interactions and activities among individuals, organisations, and systems'.

It can be characterised as a dynamic, interconnected, complex, and constantly evolving ecosystem where the forces of innovation, connectivity, and security intersect and digital interactions occur. These digital interactions take place in all the layers of cyberspace and effect dimensions (Figure 2-4). Individuals, the private sector, state entities, and all types of organisations (including terrorist and criminal organisations) operate in the cyberspace environment. It is necessary to divide the actors into state, non-state, state sponsored, and proxy and further define them as allies, neutrals, or adversaries. How they are defined affects the implementation of offensive and defensive capabilities, which requires international cooperation.

9 Hybrid activities conducted by state and non-state actors that fall below the threshold of traditional armed conflict but still seek to achieve strategic objectives through coercion, manipulation, and ambiguity.

Defining allies and adversaries is easier than defining countries that pose a hybrid threat or defining the boundaries of the private sector.[10] Therefore, a nuanced understanding of the relationships between governments, private sector entities, and other stakeholders is required in conjunction with multilateral engagement to promote cooperation and collaboration to address common cyber threats and challenges (Figure 2-4).

FIGURE 2-4: CYBERSPACE ENVIRONMENT (ŠTRUCL, 2024)



Cyberspace

Cyberspace exists within the information environment and is intrinsically linked to the electromagnetic environment.

A globally accepted definition of cyberspace does not exist. This leads to inconsistent responses of cybersecurity and defence entities at the national and international level, or between civil and military structures. There is also a difference in how cyberspace

10 In the cyberspace domain, the private sector plays a significant role, owning and operating much of the critical infrastructure and technology that underpins cyberspace. However, governments may struggle to exert influence over private-sector entities, especially multinational corporations with global operations and diverse interests.

11 (Štrucl, 2022).

is conceived of. For example, some countries do not use the term 'cyberspace', or rather, have not adopted it.[12]

- **Cyberspace (NATO definition):** 'The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data.'[13]
- **Cyberspace (European Union Agency for Cybersecurity [ENISA] definition):** 'The time dependent set of tangible and intangible assets, which store and/or transfer electronic information.'[14]

As there is no unified definition of cyberspace, **a possible unified definition** of cyberspace could be described as follows, Cyberspace is a working environment and an operational domain within the information environment consisting of a time dependent set of tangible and intangible resources, including the internet, and activities in the physical, virtual, and cognitive dimensions.[15]

Cyberspace can also be described as a domain consisting of independent but interconnected layers. The layers can be grouped according to the effect dimensions. With this model, we can achieve a comprehensive understanding of cybersecurity and cyber defence, as it is generic enough to understand and, at the same time, consistent with responding to hybrid threats with cyber capabilities and conducting multi-domain operations.

Cyberspace Operations

Cyberspace operations can be defined as: 'Actions in or through cyberspace intended to preserve own and friendly freedom of action in cyberspace and or to create effects to achieve military objectives'[16]

Historically, cyberspace operations have centred on CIS supporting mission objectives. This has evolved into cyber commands that now produce actions and effects to achieve military objectives. Full spectrum cyberspace operations consist of

12 For example, other countries' view, cyber warfare is only part of the overarching concept of information confrontation, where the terms 'information space' and 'information sphere' are used and defined as follows. 'information space', the activities associated with the formation, creation, transformation, transmission, use, and storage of information, have an impact, including individual and social consciousness, of information infrastructure and information itself. 'information sphere', a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet [...], communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating social relations in the sphere. (Stratcom_COE, 2021)

13 (NATO Standardization Office, 2025)

14 (European Union Agency for Cybersecurity, ENISA overview of cybersecurity and related terminology, 2017)

15 (Štrucl, 2025)

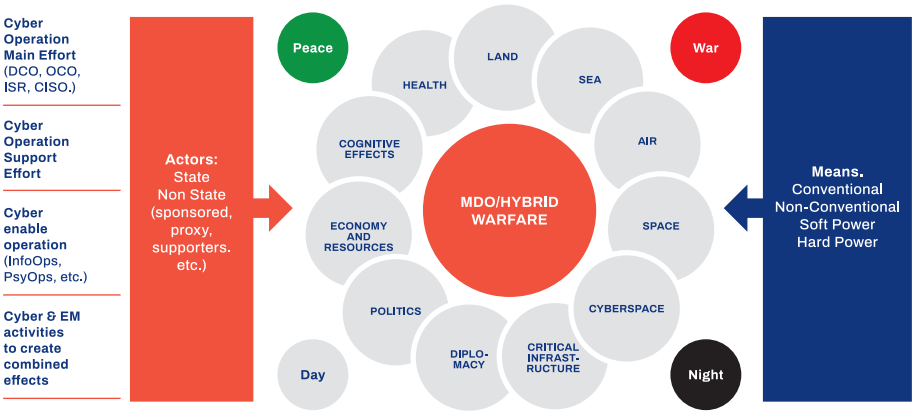
16 (NATO Standardization Office, 2025)

the following: CIS operations (CISOPS), Defensive Cyberspace operations (DCO), Cyberspace Intelligence Surveillance and Reconnaissance operations (CyISR), and Offensive Cyberspace Operations (OCO). They will be discussed further in Chapter 4. This chapter will identify the four types of mission efforts employed when conducting cyberspace operations:

- **Main effort (ME):** Cyberspace operations can be the main effort conducted in or through cyberspace to achieve specific objectives and effects. Other elements of the military can support the cyber command to achieve the main effort.[17]
- **Supporting effort (SE):** Supporting efforts are cyberspace operations which support and enhance the effectiveness of other military or security operations across different domains by providing assistance, resources, or capabilities to the main effort.
- **Cyber enabled activity (CEA):** occurs when cyber activity is integrated with other domains to achieve strategic, operational, or tactical objectives. These operations leverage cyberspace as a force multiplier to enhance the effectiveness of conventional military operations, intelligence activities, or other security efforts.
- **Cyberspace and electromagnetic activities (CEMA):** Cyberspace is intrinsically linked with the electromagnetic environment. CEMA combine cyber and electromagnetic capabilities to create effects which support the mission. It integrates the synergies between cyber and electromagnetic operations to meet the operational demands of digital and wireless communication networks in modern military operations. This convergence is essential for defending and preserving the integrity and functionality of networks in congested and contested environments, ensuring situational awareness and resilience against digital and electromagnetic threats. Additionally, the capability to monitor, detect, engage, and counter these threats enables tactical units to maintain freedom of movement and the ability to manoeuvre in highly contested areas. CEMA will be discussed further in Chapter 3.

17 The main effort is a designated subordinate unit whose mission at a given point in time is the most critical to mission success.

FIGURE 2-5: FRAMEWORK OF CYBERSPACE OPERATIONS (ŠTRUCL, 2022)



Cyber Defence

Cyber defence can be defined as: 'The means to achieve and execute defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems.'[18]

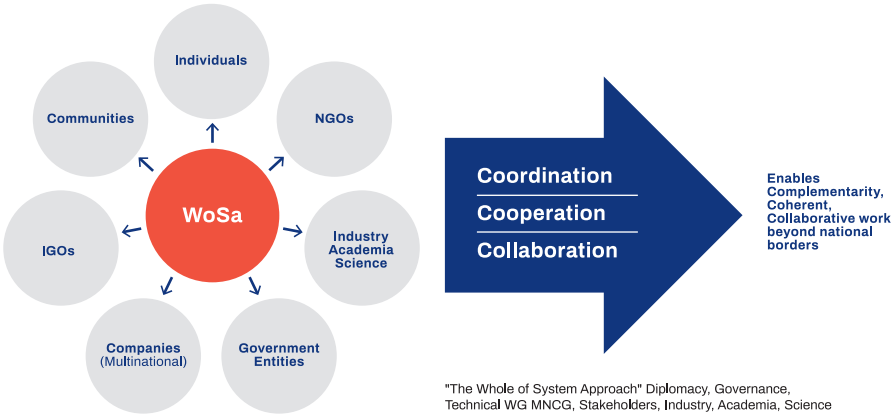
Cyber defence is intertwined with cybersecurity, and many of the actions and activities are common to both disciplines. Cybersecurity is a broad discipline aimed at safeguarding systems and networks against a wide range of threats. Cyber defence involves strategies, polices and frameworks designed to prepare and posture a government and military to defend cyberspace. It is focused on proactive and reactive measures to protect against and react to identified or potential threats. Aspects of cyber defence can be applied to all organisations; however, it is primarily a national or military concept, as there are response options and actions available to militaries which go beyond the remit of traditional cybersecurity and civilian organisations.

The contemporary security environment requires a multifaceted and all encompassing approach towards safeguarding national security and defence. Much of cyberspace is not owned or controlled by governments or the military. This necessitates cultivating security and defence capabilities that can be adapted to address a spectrum of conventional and nonconventional threats. Moreover, the delineation between cybercriminal activities and those aligned with a state's military endeavours or geopolitical objectives poses a formidable challenge. This underscores the intricate interplay between various security domains.

18 (NATO Standardization Office, 2025)

There are many key stakeholders in cyberspace. Governments[19] play a crucial role through policy, legislation, and law enforcement. The private sector, such as cybersecurity companies, service providers, and critical infrastructure stakeholders, holds much of the knowledge and response capability. Industry and academia play a vital role in cyberspace, providing the research, technological advances, and expertise necessary to effectively address cyber threats. It is paramount to acknowledge the predominant ownership of cyberspace by the private sector, and it is crucial to recognise the military's expertise in crisis response and logistics. Establishing a whole-of-society (WoS) and whole-of-system approach (WoSa)[20] encompassing all stakeholders becomes necessary. Through coordination, cooperation, and collaboration, this approach facilitates synergy, coherence, and collaborative responses, extending beyond national boundaries.

FIGURE 2-6: THE WHOLE-OF-SYSTEM APPROACH (ŠTRUCL, 2024; ADOPTED FROM KLIMBURG, 2012)



The Transition of Cyber Defence from Peace Through Crises and Conflict

A NATO CCDCOE analysis found that the role of the military in the EU and NATO member states in peacetime was limited to the cyber defence of the military CIS.[21] In some cases, highly specialised assistance is given to the civil authorities. Although such an approach is understandable in peacetime, it must be taken into account that no defence is carried out with solely military or solely civilian capabilities. It is necessary to establish a structure in peacetime that will enable public-private partnerships in

19 The term 'government' here refers to the whole state apparatus: the legislative, executive, and judicial branches, including all other state bodies.

20 The whole-of-society approach emphasises collective responsibility for cybersecurity by engaging governments, businesses, civil society, and individuals to create a culture of awareness, collaboration, and shared action. The whole-of-system approach focuses on integrating and coordinating all components of the cybersecurity ecosystem to build a resilient and adaptive defence. (Klimburg, 2012)

21 (Štrucl, 2022).

peace, crisis, and conflict. Key terrain cyber (KT-C) and mission-vital infrastructure cyber (MVI-C) (defined in Chapter 3) will often include cyberspace not controlled or operated by the military. Therefore, in times of crises and conflict, militaries will have an interest in relevant cyberspace not directly owned or operated by them but is important to the mission.

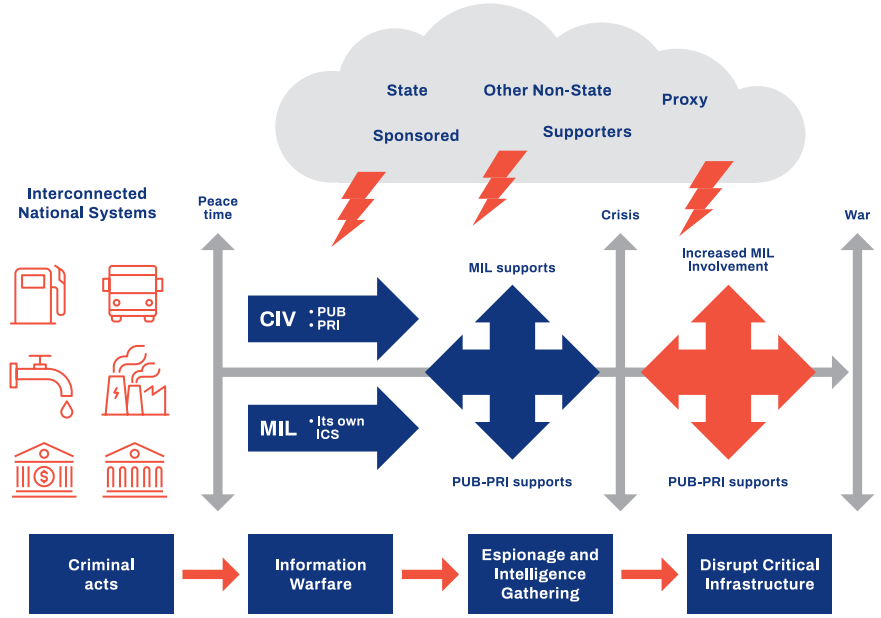
Acknowledging the operational continuum characterising cyberspace, many initiatives at the EU or NATO[22] level support civil-military mechanisms and processes of transition from peacetime through crisis to conflict. Examples of these initiatives are the NATO Virtual Cyber Incident Response Capability (VCISC) and the EU permanent structured cooperation (PESCO) cyber rapid response teams and mutual assistance in cybersecurity (CRRT).

When planning and implementing security and defence activities, it is important to take into account the whole-of-society and whole-of-system approach (Figure 2-7). Roles and responsibilities need to be assigned to national security and defence structures, including public-private partnerships and relevant memorandums of understanding. Known as 'total defence' or 'integrated defence', this approach establishes synergy in cyber defence. It facilitates defence activity establishing command and control with military, public, and private structures,[23] including individuals who have the appropriate skills. Establishing this structure in peacetime ensures a quick and agile response in any circumstance, be it peace, crisis, or war.

22 David Van Weel, NATO assistant secretary general for emerging security challenges, told the 15th International Conference on Cyber Conflict (CyCon) 2023, 'We need to strengthen the role of our military cyber defenders during peacetime. And this is important because in most national contexts, the military only gets involved during crisis and conflict'. He went on to say that 'cyberspace is never fully at peace, there is a constant friction, and we have to prevent scenarios where we expect our militaries to perform some kind of magic handover to take over without having been in the room for the lead-up to the crisis'. https://therecord.media/nato-peacetime-cyberdefense-david-van-weel-cycon

23 These include bilateral agreements with non governmental organisations (NGOs) and intergovernmental organisation (IGOs), national and international corporations, individual experts, and academia.

FIGURE 2-7: THE WHOLE-OF-SOCIETY APPROACH (ŠTRUCL, 2024; ADOPTED FROM STEINGARTNER, GALINEC, KOZINA, 2021, P. 5)



2.3 THREAT LANDSCAPE

Cyberattacks can be invisible, asymmetric, multi-role, deniable, global, and instantaneous, which makes cyberspace an ideal environment for big and small actors alike. The threat landscape encompasses the recognised and potential cyber threats and is a dynamic environment that changes continuously. Increasingly sophisticated adversary behaviours, and technological advances require a comprehensive understanding of the operational environment and the organisational attack surface. Additionally, even unintended factors such as errors or environmental conditions can significantly disrupt the system functionality, impacting critical services.[24]

The cyberspace threat landscape is vast and requires constant review and analysis. As it is not possible to present the full cyberspace threat landscape in this handbook, some relevant concepts are presented here. There are numerous avenues available to the cyber commander to receive information on the threat landscape, such as own infrastructure log analysis, open source threat reports, commercial threat reports, computer emergency response team (CERT) reports, information sharing arrangements, and military intelligence. New technologies act as force multipliers

24 (National Cyber Security Centre Ireland, 2022)

by facilitating highly targeted and evasive attacks in conjunction with conventional tactics, techniques, and procedures. This makes it imperative that cyber commanders' combine all available information to provide the context vital for understanding the cyberspace threat.

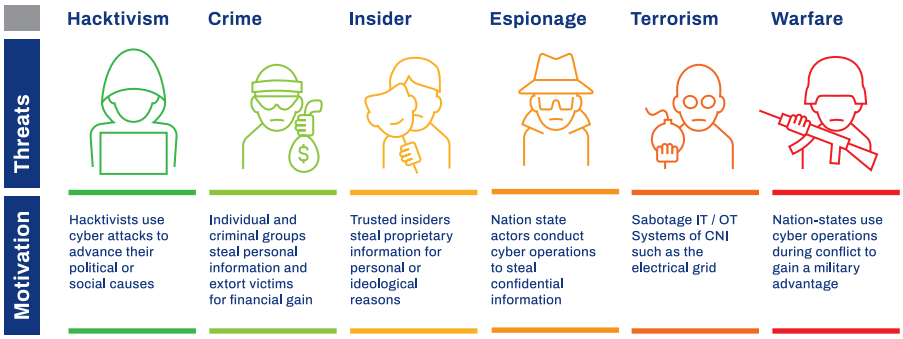
Tactics, Techniques, and Procedures (TTPs):

- **Tactics:** The highest level description of the threat actor's behaviour.
- **Techniques:** Methods used by the threat actor in the attack.
- **Procedures:** Actions taken by the adversary that seek to establish the conditions to successfully conduct the cyberattack, such as a brute force attack, social engineering, or malicious software.

TTPs can be used to correlate an attack to a known threat actor and to understand the possible attack frameworks. This understanding supports security and defensive actions, as well as the attribution process.

Threat actors: A wide variety of actors are operating in cyberspace (Figure 2-8), including one's own forces, friendly forces, neutrals, and adversaries. Any of these can be actual or potential threats.

FIGURE 2-8 IDENTIFIES THE MAIN CATEGORIES OF THREAT ACTORS, WHICH ARE DESCRIBED IN GREATER DETAIL BELOW.



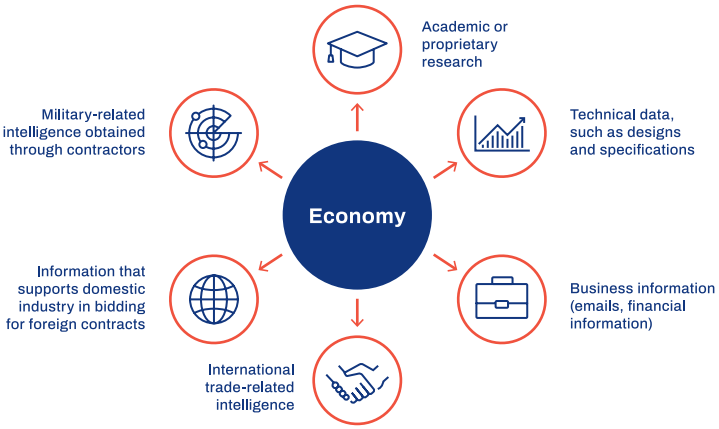
State Actors

State actors: These actors are characterised by geopolitical, economic, and/or military motivations. They are well resourced and possibly the most dangerous. They are capable of launching enduring and/or sophisticated attacks, often for espionage, sabotage, impact on the cognitive environment, or to disrupt or deny cyberspace in order to gain a strategic and/or economic advantage. Nation states may conduct cyberspace operations directly or through proxies.

State proxies: Often referred to as advanced persistent threats (APT), these are well funded and resourced organisations or groups with advanced capabilities. They are generally involved in espionage or revenue generation and usually controlled by a state apparatus within a nation state, i.e. the military or an intelligence service. Well resourced APTs conduct complex, far reaching, and sophisticated malicious activities, designed for prolonged intrusion to achieve their objectives. State proxies support governments' geopolitical, economic or military objectives which may include but not limited to the following:

- **Disruption and sabotage:** State-sponsored groups are increasingly demonstrating and refining their capabilities for disruptive operations, including the spillover effect. Critical national infrastructure and operators of essential services are key areas of interest for adversary cyberspace activity.
- **Espionage:** Espionage by state actors and state-sponsored actors poses a significant threat to the sovereignty of all nations. States can use cyberspace to spy in order to gain strategic and economic advantages.[25]

FIGURE 2-9 TARGETS OF INTEREST FOR ESPIONAGE THROUGH CYBERSPACE.



Non State Actors

Cyberterrorists: Groups or individuals who attack or influence CIS and information, especially against civilians, by spreading terror for political aims.

Cybercriminals: Criminal groups driven by profits. They are typically looking for personally identifiable information (PII), critical digital resources to hijack for ransom, or ways to bring their existing criminal activities online, such as cybercrime as a service.

25 (Canadian_Centre_for_Cybersecurity, National Cyber Threat Assessment, ISSN 2816-9182, 2024).

Hacktivists: Individuals who adhere to a specific cause or ideology and who seek to spread propaganda or cause an impact in the cognitive environment to damage entities and/or organisations to which they are opposed.

Insider threats: Individuals working from within their own organisation who use their authorised access, intentionally or unintentionally, to harm the department's mission, resources, personnel, facilities, information, or CIS. Insider threats manifest themselves in various ways: violence, espionage, sabotage, theft, and cyber acts. Three elements define an insider threat: 1) privileged access to organisational assets, 2) intent, malicious or otherwise, and 3) potential to harm an organisation. Consequently, the insider threat is the circumstance that enables the incident, and while not needed to define an insider threat, the cyber dimension definitively increases the threat's potential.

- **Unintentional threats:** Non malicious (frequently accidental or inadvertent) exposures of an organisation's CIS infrastructure, systems, and information that cause unintended harm to an organisation.
- **Intentional threats:** Malicious actions performed by malicious insiders who use technical means to disrupt or halt an organisation's regular business operations, identify CIS weaknesses, gain protected information, or otherwise advance an attack plan via access to CIS. This action can involve changing data or inserting malware or other pieces of offensive software to disrupt CIS.

Threat actors do not always fit neatly into these categories for various reasons. For instance, some nation states conduct both espionage and cybercrime, and some cybercriminals provide cyberspace operations as a service to the highest bidder. As tactics, techniques, and procedures apply across multiple behaviours, and similar behaviours apply across multiple actors, it is extremely difficult to codify the type of actors involved.

The intent of the threat actor is not always clear from the beginning. Moreover, there is no clear demarcation between, for instance, criminal activities, terrorism, espionage, and a military operation. So all possible legal authorities, including those in the civilian sector, should cooperate and share information as early as possible when conducting cyberspace operations.

Cyberspace Attack Vectors

Cyberspace attack vectors are methods used to infiltrate a victim's CIS. Increasingly, artificial intelligence (AI) is being used to create the payloads for these attack vectors. All types of CIS, including air gapped networks, can be vulnerable to cyberspace attack

vectors. These vectors allow attackers to exploit vulnerabilities in CIS infrastructure, gaining unauthorised access to sensitive data and potentially compromising the confidentiality, integrity, and availability (CIA) of mission critical systems and vital infrastructure. Understanding a variety of attack vectors is essential for defending against adversary actions, identifying adversary capabilities, and achieving mission assurance.

- **Attack vector:** This is the route or method an adversary uses to gain unauthorised access to a CIS. Attack vectors can be delivered through a phishing email, by visiting a compromised website, or by obtaining physical access to a network that can exploit vulnerabilities in software, operating systems, or network protocols.
- **Payload:** The malicious software that exploits the vulnerabilities and enables the threat actor to establish a foothold and interact with the target.
- **Living off the land (LotL):**[26] This is a file less malware cyberattack technique where the cybercriminal uses native, legitimate tools within the victim's system to sustain and advance an attack.
- **Effects:** The intended outcomes of the cyberspace operations. They are most often virtual but may be physical.
- **Denial of service (DoS):** An attack that denies access to a legitimate CIS or network resources. DoS typically occurs by flooding the target host with network traffic, overloading the host's ability to respond.
- **Distributed denial of service (DDoS):** DDoS refers to a situation when multiple machines work together to deny access to the CIS or resource. DDoS often use botnets to achieve their aim.
- **Social engineering:** The act of deceiving an individual into revealing sensitive information, obtaining unauthorised access, or committing fraud by associating with the individual to gain confidence and trust.[27]
- **Supply chain attacks:** Threat actors may compromise the supply chain if suppliers have vulnerabilities in their security measures. Compromised software or hardware can allow an adversary to gain unauthorised access to data and or information, leading to data theft, manipulation, and disruption of operations.

2.4 TRENDS SHAPING THE THREAT LANDSCAPE

Artificial intelligence (AI): AI is amplifying cyber threats by lowering the barrier of entry and the necessary scale and sophistication of malicious cybers activities. Cybercriminals and state sponsored actors are leveraging AI tools such as large language models (LLMs) when creating social engineering, deepfakes, and personalised phishing attacks. AI is being used to automate cyberattacks, thereby

26 (Lenaerts-Bergmans, 2023)
27 (NIST, 2008)

reducing the human element. Deepfakes undermine trust, polarise societies, and spread misinformation.[28]

Cyberspace threat actors: These actors are adapting their TTPs to evade detection by targeting 'edge' devices, exploiting vulnerabilities, and using stealthy techniques like 'living off the land'. Additionally, they misuse domestic infrastructure, such as small office/home routers, to blend malicious activities into normal traffic.

Geopolitical conflicts: Non-state actors are conducting disruptive cyberattacks like DDoS and defacements, often targeting critical infrastructure. These actors operate in unpredictable ways, motivated by patriotism, ideology, or notoriety.

Vendor concentration: Reliance on a few dominant technology vendors increases vulnerabilities. Attacks on major providers, such as cloud services, can have cascading effects on entire sectors and national security. Cyberspace threat actors can target these providers to exploit weaknesses and access sensitive data.

2.5 NATIONAL CYBERSPACE ACTORS

Cyberspace is a complex environment that affects every layer of our society. This is why many different interdependent actors have been assigned roles and responsibilities in cyberspace operations at the national level. In order to fulfil their role effectively, these actors need to be aware of the others' areas of governance and mandates. Although the structures and organisations assigned roles and responsibilities in cyberspace vary from nation to nation, a general framework with corresponding roles is outlined below:

- **National cybersecurity centre:** Most nations have an entity that is responsible for national cyberspace and that pays particular attention to critical national infrastructure (CNI). The main purpose of this entity is to inform legislation; to detect, observe, and analyse online security problems; and to inform the public. Generally, a national computer emergency response team (CERT)[29] is established to provide assistance to public and private entities affected by cyber incidents.
- **Law enforcement:** The responsibility for crime prevention, apprehension, and prosecution lies in the hands of national law enforcement. During a cyberattack, the complete scope and true intentions of the threat actor are generally unclear. So cyberattacks should always be considered possible criminal acts, and law enforcement agencies should be involved as soon as possible.

28 (Canadian_Centre_for_Cybersecurity, National Cyber Threat Assesment , ISSN 2816-9174, 2025)
29 This type of organization may also be called CIRT or CSIRT.

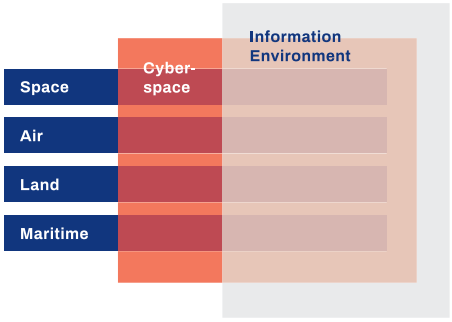
- **Military.** The role of the military in cyberspace is to contribute to the defence of the nation against external threats. Within the military community, three cyberspace operations authorities can usually be identified:
    - **Cyber command:** The cyber command executes the delivery of the four types of cyberspace operations: CIS Operations (CISOPS), Defensive Cyberspace Operations (DCO), Cyberspace ISR (CyISR), and Offensive Cyberspace Operations (OCO). When conducting cyberspace operations, cyber command ensures the delivery of actions and effects required by the mission to ensure mission assurance and national cyber defence.
    - **Military police:** The military police are responsible for cybercrime investigations within military installations.
    - **Military intelligence:** Military intelligence plays an important role in cyber threat identification, counterintelligence, and the cyber targeting process in support of military operations.
- **Intelligence community:** The intelligence community is responsible for the collection and analysis of cyber threat intelligence in order to reduce national security risks with regard to terrorism, espionage, subversion, sabotage, and organised crime. The cyber command needs to have properly established information sharing mechanisms in place, not only with military intelligence but also with all other intelligence entities, since each of them might have different information at their disposal.
- **Private sector:** The private sector consists of both national and international companies. The private sector plays an important role, since the majority of internet service providers (ISPs), digital service providers (DSPs), critical information infrastructure (CII), and critical national infrastructure (CNI) are in private hands. The cyber command will often act through private ISP networks or be required to defend private CII/CNI. The private sector is responsible for the security of its own infrastructure and for cooperating with state institutions to promote cybersecurity and to enable cyberspace operations where needed.
- **International environment:** International institutions are mainly responsible for the creation of international rules and regulations and for the coordination and deconfliction of cyberspace operations' efforts in case of multinational projects or military campaigns.

3. Cyberspace as a Domain of Operations

'Cyberspace is not special, but it is different.' The concepts and ideas that are already well established in other domains of operations of land, sea, air, and space can also be applied to the cyberspace domain. It is an ever changing environment built by humans, and it is utilised by the military and civilians. Parts of cyberspace that the military and governments rely on are owned and controlled by private industry and vice versa. Ultimately, cyberspace is operated and used by all operational domains.

Cyberspace operations deliver actions and effects that can create decisive conditions,[30] directly supporting mission assurance. Cyber actions take place in one or more of the seven layers of cyberspace, and the effects occur in one or more of the three effect dimensions. In addition, cyberspace is an element of the engagement space.[31] These operations leverage cyber capabilities to generate tactical effects or achieve strategic impacts. Conducting operations in cyberspace requires a mission focused mindset. The effects produced in cyberspace support activities in other domains, just as other domains can support the cyberspace domain in achieving its mission. For example, during a joint operation, land forces could sever an adversary's communication cables, denying the adversary freedom of movement in cyberspace and reducing its ability to communicate. Therefore, it is essential to integrate cyber considerations into the planning process as early as possible.

FIGURE 3-1: 21ST CENTURY BATTLESPACE DOMAINS AND THE INFORMATION ENVIRONMENT



30 A decisive condition is a combination of circumstances or effects or a specific key event, critical factor, or function that, when achieved, allows commanders' to gain a marked advantage over an opponent or contribute materially to achieving an objective

31 Engagement space: The part of the operating environment where actions and activities are planned and conducted

No offensive or defensive capability remains effective indefinitely. Cyberspace is less geographically constrained than physical domains. Cyberspace infrastructure has a physical location and identifiable electronic boundaries. Cloud computing and hyper connectivity provide accessibility to anyone with the appropriate knowledge and technology. Where boundaries do apply, they are within certain contexts, such as national responsibilities and jurisdiction. The simultaneous use of specific cyberspace components by adversaries, allies, neutral parties, and other elements may significantly complicate the achievement of mission objectives in cyberspace.

Cyberspace and the electromagnetic environment (EME) are increasingly interconnected, with cyberspace operations often relying on the EME. As they become more intertwined, an integrated approach is needed to manage the EME and cyberspace as distinct yet complementary objectives. This requires a comprehensive approach addressing resources, doctrine, and strategy. Military success now heavily depends on dominance in the EME.

Furthermore, cyberspace is a facilitator for the transfer, storage, and consumption of data, information, and knowledge and, therefore, has a direct linkage to the information environment. Unlike in the kinetic domains, small–scale actors can make a large impact and reach parity with larger actors in cyberspace. The underlying technologies and protocols of cyberspace enable both legitimate and malicious activities.

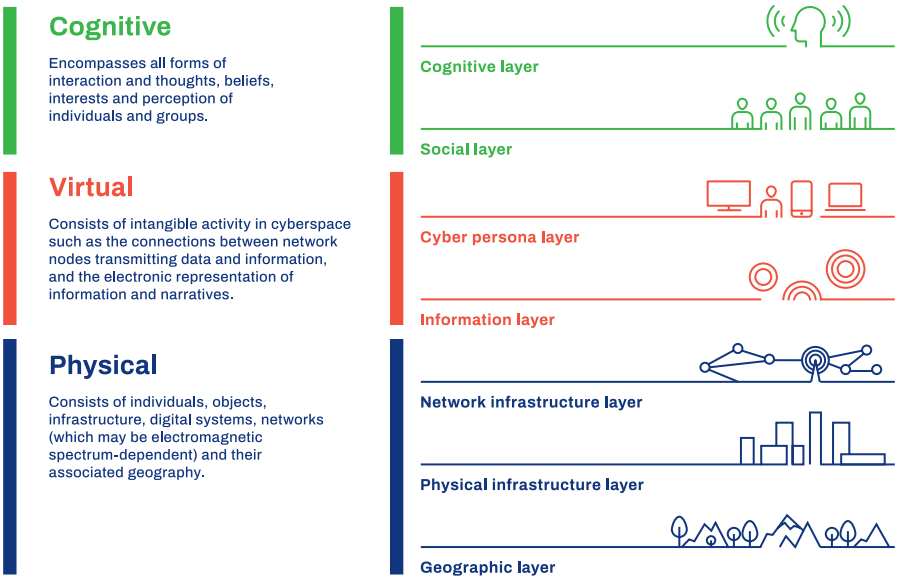
Adversaries exploit and weaponise vulnerabilities to steal intellectual property, manipulate information, and create malicious software capable of disrupting or destroying systems in order to gain a strategic advantage. Nations must increase their resilience, defend in depth, demand security by design, and persistently detect and engage cyberspace threat actors, disrupting their freedom of action in blue cyberspace. Cyber events can occur at any time. Increases in the number of events in cyberspace can indicate potential threats and risks. When analysed with other intelligence sources, they may indicate shaping activities in advance of a kinetic attack.

Although the details of the principle of sovereignty in relation to cyberspace are still discussed among nations, some parts of this principle seem to be settled: no nation can claim overall sovereignty over cyberspace; there is sovereign equality among the nations; and sovereignty includes exclusive authority over territory, individuals, and physical assets. This leads to the situation in the cyber context in which sovereign control can be executed only over (physical) cyberspace infrastructure that is located within the borders of a nation.

3.1 THE LAYERS OF CYBERSPACE

Cyberspace has often been described as having three layers. However, that approach made it difficult to target or separate some aspects of cyberspace. Increasingly, a seven layer model (Figure 3-2) of cyberspace is being adopted.[32] These seven layers can be categorised into three distinct effect dimensions: physical, virtual, and cognitive. An effect dimension is 'an analytical construct that translates actions in the engagement space into the physical, virtual and cognitive consequences that these actions may have'.[33] When conducting cyberspace operations, actions occur in one or more of the seven layers, and the effect takes place in the effect dimensions. The layers of cyberspace build upon each other, and operations in and through cyberspace can involve any combination of the seven layers.

FIGURE 3-2: THE SEVEN LAYERS OF CYBERSPACE AND THE EFFECT DIMENSIONS



The cognitive effect dimension includes the following two layers (Cognitive, Social)

Cognitive Layer

The cognitive layer reflects intangible characteristics such as the human psyche, will, attitude, thought, and understanding, which in turn are shaped by the social layer. The cognitive layer gives rise to perception and, in turn, represents how people make sense of a situation. Cognitive influence therefore plays a key role in shaping actions

32 (NATO AJP 3.20 Study draft 1, Mar 2025).
33 (NATO Standardization Office, 2025).

and is a vital consideration for targeting, particularly in terms of information based operations.

Social Layer

The social layer serves to analyse the groups, audiences, and relationships that people form. These relationships influence how people act and therefore have a direct correlation to the cognitive layer.

The virtual effect dimension includes the following two layers (Cyber Persona, Information)

Cyber Persona Layer

The cyber persona layer consists not of real persons or organisations but of representations of their virtual identities. A virtual identity can be an email address, user identification, social media account, or alias. Consequently, one person or one organisation can have multiple cyber personas. Conversely, multiple people or organisations can also create a single, shared cyber persona.

Information Layer

The information layer in previous texts was referred to as the logical layer – is intangible. It includes code, data, firmware, operating systems, user applications, network configurations, protocols which govern the transfer of data and information, and other software and data components. The information layer cannot function without the physical and network infrastructure layer since information flows through wired networks or the electromagnetic spectrum (EMS).

The physical effect dimension includes the following three layers (Network Infrastructure, Physical Infrastructure, Geographic)

Network Infrastructure Layer

The network infrastructure layer comprises the physical elements of a cyber system or network, such as computer hardware, network infrastructure, cabling, and CIS infrastructure. Notably, in this layer, the electromagnetic spectrum (EMS), as well as the cabling wired communication, bridges the information and network infrastructure layers. The EMS enables the transmission of intangible elements, such as data and protocols, within the information layer while also functioning as a physical medium in the network infrastructure layer, similar to how cables support wired communication. Thus, the EMS facilitates the flow of information across both layers.

Physical Infrastructure Layer

The physical infrastructure layer relates to tangible objects that may have an association with cyberspace and, by extension, its functionality but do not form a component part of the actual network. Examples include people, buildings, and vehicles.

Geographic Layer

The geographic layer represents the location where elements of the physical and network infrastructure layers are found.

3.2 CYBERSPACE ZONES

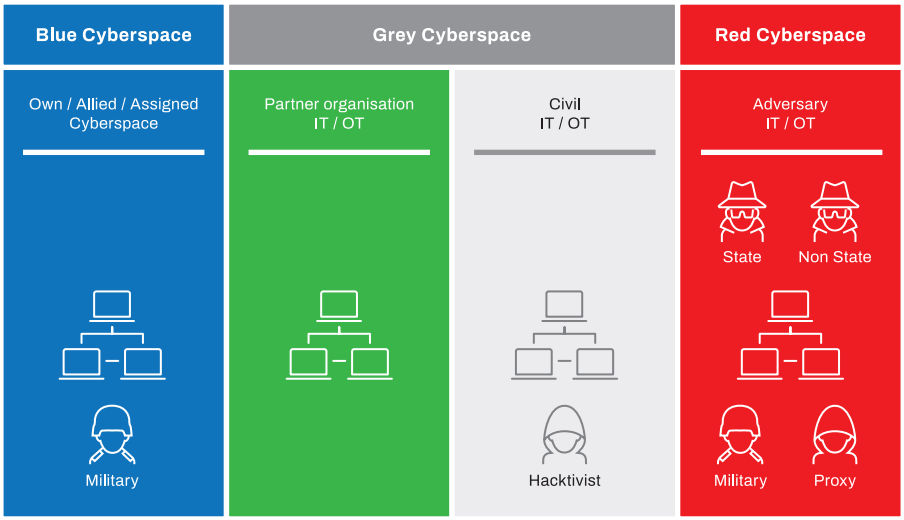
To simplify cyberspace operations planning and execution, the cyberspace terrain can be divided into different zones (Table 3-1), which are based on the entity that controls and operates the terrain. The zones are designated using different colours. During the different phases of the continuum of competition, the responsibility over different parts of cyberspace may change, which can change the colour of zones.

The system of cyberspace zones uses different colours to differentiate between adversarial, friendly, and neutral zones.

TABLE 3-1 CYBERSPACE ZONES

Cyberspace zones	Colour	Description
Own/Assigned	Blue	Own military/government/critical infrastructure, owned, operated and protected cyberspace vital to the mission.
Neutral	Grey	All cyberspace that does not meet the description of blue or red. Contains two sub-categories: green and white.
Partners	Green	Partner militaries / government-owned, -operated, and -protected cyberspace.
Public IT/OT infrastructure	White	Public cyberspace that is not in blue, green, or red cyberspace. Elements of white cyberspace may be vital to the mission.
Adversary	Red	Cyberspace owned, controlled, and protected by an adversary

FIGURE 3-3: CYBERSPACE ZONES



Delineating different zones in cyberspace is challenging, because various actors can occupy the same cyberspace terrain without being aware of each other. Unlike physical domains, which have clear geographical boundaries, cyberspace is increasingly virtualised, borderless, and ever changing. This makes it difficult to assign specific areas to specific actors. The rapid evolution of technology, tactics, techniques, and procedures further blurs the lines between these actors. The anonymity that cyberspace offers adds to this complexity.

When military forces manoeuvre in neutral or adversary cyberspace, national and/or international rules and regulations may require a specific approach that depends on which state the cyberspace infrastructure is located in. When cyberspace zones are used in a visual format, the approach must include country boundaries.

The grey zone is any cyberspace that is not blue or red. The grey zone is not homogenous and contains two types of areas of interest that are important for a cyber commander. These subcategories are designated green and white. Green is used for partner owned, operated, and protected cyberspace, and white is used for public IT/OT infrastructure. The green and white areas do not constitute the entirety of the grey zone. Grey zone cyberspace can be, but is not limited to, economic, social, political, critical national infrastructure (CNI), or operators of essential services. Cyber activities such as espionage, information warfare, and disruptive attacks in this zone can have a significant political, economic, or security impact. Non-state actors and

proxies often operate in the grey zone, which can increase the challenges associated with attribution, counteractions, and rules of engagement.

3.3 CYBERSPACE AND MULTI-DOMAIN OPERATIONS (MDO)

MDO (NATO definition): 'The orchestration of military activities across all operational domains and environments, synchronised with non-military activities to enable the alliance to create converging effects at the speed of relevance.'[34]

MDO (US Army definition): 'Multi-domain operations are the combined arms employment of joint and Army capabilities to create and exploit relative advantages that achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force commander.'[35]

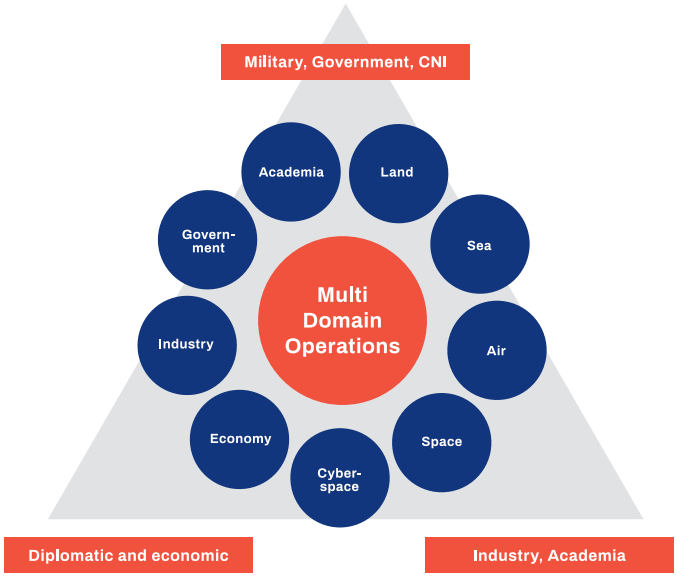
Multi-domain operations is a term that, despite its ubiquity in military literature and increasing prevalence in doctrine, remains ambiguous and contested.[36] MDO operations, at their core, synchronise and orchestrate activities across all domains to achieve complementary and reinforcing effects. MDO emphasises a comprehensive focus across all domains, which ensures that convergence is achieved, allowing effects from all domains, including cyberspace, to be integrated and synchronised. MDO extends to military and non military instruments of power, making it broader and more integrated (Figure 3-4).

NATO's vision for MDO integrates military and non military instruments of power, including diplomacy and economic measures, allowing a unified and coordinated response. Collaboration with partners and stakeholders, including private industry, academia, and partner nations, drives technological innovation and strengthens operational capabilities.

When conducting cyberspace operations, the staff will have to plan for and operate alongside a broad range of actors and entities. These include other branches and services of the military, government agencies, operators of critical infrastructure, internet service providers, IT service providers, cybersecurity companies, and academia. To ensure effective integration of cyberspace into MDO, it is essential that collaboration, cooperation, and memorandum of understanding (MoU) are established across the full range of actors and entities during peace, crises, and conflict.

34 (NATO Standardization Office, 2025)
35 (Department of the army, FM 3 0perations, 2022)
36 (Bower Ian, 2024)

FIGURE 3-4: MDO CONCEPT



Some cyber considerations for multi-domain operations that the Joint Force Command (JFC) should consider are as follows:

- Adversary operations in cyberspace that may affect the mission, including command and control.
- Cyberspace assets available to the cyber commander (organic and non organic) and the operational constraints, if any.
- Capabilities of friendly forces and the adversary to conduct CISOPS, DCO, CyISR, and OCO.
- Considerations for interagency coordination, deconfliction, and synchronisation and the relevant time factors.
- Appropriate legal frameworks.

3.4 CYBERSPACE AND ELECTROMAGNETIC ACTIVITIES (CEMA)

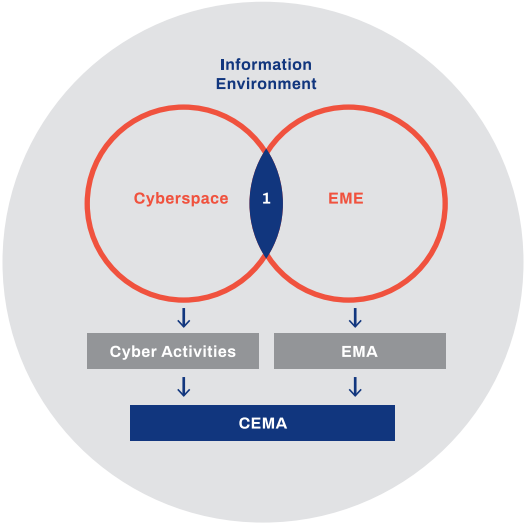
By integrating and synchronising cyberspace operations and EW, friendly forces gain an information advantage across multiple domains and lines of operations.[37]

37 (Department of the army, FM3-12 CEMA, 2021).

Although electronic warfare is outside the scope of this publication, it is important to note that cyberspace and the electromagnetic environment (EME) are now interdependent and linked.[38] A section of cyberspace operates in or through the EME. Both environments are contested, and actors will use cyber and electromagnetic activities to gain an operational advantage. Given our reliance on the modern digital environment, coordinating CEMA is essential for operational success. The ability to create effects through coordinated CEMA provides a significant advantage. Understanding the interdependencies of identified key terrain cyber (KT-C) with the EME will enhance the defence of friendly cyberspace and inform military response options in cyberspace.

Cyberspace and the electromagnetic environment are linked through the physical and network infrastructure layer (Figure 3-5). A section of cyberspace depends on the electromagnetic spectrum for communication, through devices such as wireless networks, satellites, microwave infrastructure, and fibre optic cables. Cyberspace is influenced by electromagnetic activities where the electromagnetic spectrum can be congested, jammed, or spoofed. The electromagnetic spectrum can be influenced by activities in cyberspace, whereby electromagnetic signals can be generated by the processing of data.[39]

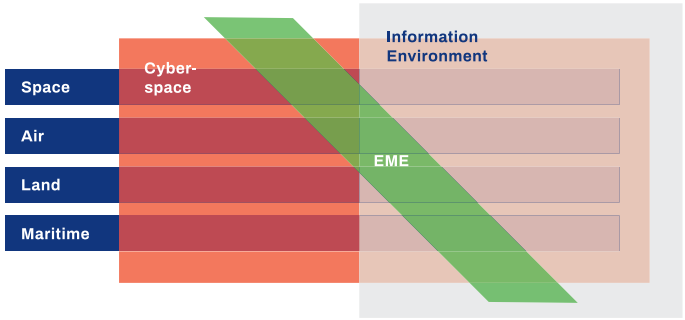
FIGURE 3-5: RELATIONSHIP BETWEEN CYBERSPACE AND THE EME



1. Physical Infrastructure Layer

38 (UK MOD, 2018))
39 (Arghire, 2024)

FIGURE 3-6: RELATIONSHIP BETWEEN INFORMATION ENVIRONMENT, OPERATIONAL DOMAINS, AND THE EME



3.5 CYBERSPACE AREAS OF OPERATION

While it is difficult to identify exact locations and boundaries in cyberspace definitively, it is useful to draw parallels from traditional domains for planning purposes. In doing so, actions taken in cyberspace will contribute to unity of effort and unity of purpose for cyberspace forces. We must start by defining our areas of interest, areas of operation and areas of responsibility.

Areas of Interest (AoI)

Areas of interest refers to the geospatial area or systems node or link against which information that will satisfy a specific information requirement can be collected.[40] The AoI in cyberspace is where information and intelligence can be used to understand friendly and adversary capabilities and intent. The cyberspace AoI is often wider than the physical operations area.

Area of Operation (AoO)

The cyberspace area of operation consists of connected and independent networks and systems; it intersects with all the other domains and can be global in reach.

Area of Responsibility (AoR)

The cyberspace area of responsibility refers to the areas in cyberspace which are designated to particular units and sub-units where they have the authority to plan and conduct operations.

40 (Department of the army, FM3-12 CEMA, 2021)

3.6 TERRAIN ANALYSIS IN CYBERSPACE

Describing cyberspace in terms of terrain is crucial for understanding it and identifying the elements that support and enable the mission. In addition, such a description allows planners to use concepts that are well established in other domains for terrain analysis. This perspective includes the cyberspace zones and effect dimensions. The unique nature of cloud services must also be understood to develop a thorough terrain analysis. As cyberspace is often not owned by governments or the military, liaisons must be established between relevant actors to develop knowledge and understanding of relevant cyberspace terrain.

On completion of the terrain analysis, areas of cyberspace may be identified that are relevant and important to the mission but are not controlled by the military or government. Mapping all of cyberspace is impossible. Therefore, the identification of these assets will allow planners to focus on what infrastructure is important to the mission, discover the vulnerabilities, and ultimately manoeuvre cyberspace forces to conduct cyberspace operations in order to achieve the mission.

Incorporating the electromagnetic environment into terrain analysis enhances the capability to conduct cyberspace operations and facilitates coordination across the operational domains, where electromagnetic spectrum use is essential. This approach allows for better strategic and tactical decision making, optimising the positioning of assets, maintaining communication, and avoiding vulnerabilities. Additionally, analysing the EME helps identify potential weaknesses in communication linkages and edge services, improving their reliability and integrity.[41]

Once completed, the terrain analysis supports the development of products such as the cyber prioritised asset list (CPAL) and the development of target lists. A cyber prioritised asset list is ‘a list of prioritised critical assets essential to the mission. They are identified through the cyberspace terrain analysis process. It is a continuous process which identifies mission vital infrastructure cyber, critical national infrastructure, and key terrain cyber. The CPAL must be reviewed on a regular basis to ensure that the most up to date information is available to planners and decision makers.

The principles of traditional terrain analysis can also apply when planning cyberspace operations. They can include the following concepts.

Obstacles

Obstacles in cyberspace refer to the use of any technology that prevents, restricts, or delays movement. This can be achieved through activities such as the deployment of

41 (NATO AJP 3.20 Study draft 1, Mar 2025)

firewalls, intrusion detection and prevention systems, principles of least privilege, and application whitelisting.

Cover and Concealment

Cover and concealment is protection from adversary observation and surveillance. In cyberspace, this can be achieved, for instance, through the use of encryption or a virtual private network (VPN).

Observation and Fields of Fire

Observation is the ability to see friendly and adversary actions and key aspects of the terrain in order to judge strength and respond to threats.[42] In cyberspace, this can be achieved through activities such as monitoring and reviewing network activity, analysing malware, reviewing adversary TTPs.

Avenues of Approach (AoA)

Avenues of approach is a relatively unobstructed route that leads to an objective of key terrain. Identifying how different aspects of cyberspace are connected will allow a planner to describe possible routes that you or the adversary will have to move through. In cyberspace, this can be, for instance, an internet service provider (ISP) entry point or a communication link between two points.

Key Terrain Cyber (KT-C)

Similar to other domains, key terrain cyber is any cyberspace whose seisure, retention, or disruption affords a marked advantage to an attacker or defender.[43] Identifying key terrain cyber allows planners to optimise their efforts and position cyberspace forces effectively to achieve the mission. In blue cyberspace, this aids in creating the cyber prioritised asset list (CPAL), prioritising defence and resilience. In red cyberspace, it supports target list development. Additionally, understanding key terrain cyber helps determine how cyber events in cyberspace can impact the mission and informs response options.

Mission Relevant Terrain Cyber (MRT-C)

MRT-C refers to areas in cyberspace that support a specific military mission or objective. It is a subset of key terrain cyber. MRT-C may change as the mission progresses or changes focus. MRT-C can exist outside government or military owned blue cyberspace.

Both KT-C and MRT-C can be identified by examining the mission, defining the capabilities that contribute to mission success, and identifying the cyberspace systems that underpin those capabilities.

42 (Raymond, Conti, Cross, & and Michael Nowatkowski, 2014).
43 (Raymond, Conti, Cross, & and Michael Nowatkowski, 2014)

Mission-Vital Infrastructure (MVI-C)

Mission vital infrastructure cyber refers to assets, systems, and networks that are essential for the successful execution of military operations.

Limit of Exploitation (LoE)

The limit of exploitation is a line beyond which subordinate commanders' must not exploit the success of earlier stages of an attack.[44] An objective in cyberspace can be a physical device or a logical location such as a system, application, or service. This helps to orientate the cyberspace operations and provide a unity of purpose and unity of effort. Once the objective has been set, a limit of exploitation or limit of advance (LoA) can be set, as further advance may become counterproductive. Due to the virtualised and interconnected nature of cyberspace, it can be difficult to set a definitive limit of exploitation or limit of advance. In CISOPS or DCO, an LoA may be the edge of your assigned cyberspace, and in OCO, the LoE may be achieving persistence in the target of interest.

3.7 USING TERRAIN ANALYSIS TO UNDERSTAND THE CYBER BATTLESPACE

Defending your territory through DCO can be enhancing the confidentiality, integrity, and availability (CIA) of your cyberspace assets. It involves identifying critical systems, pinpointing weaknesses, and setting up plans to identify and counter threats.

Keeping information flowing through CISOPS can be maintaining reliable communication and data systems. This means ensuring that information is accurate, accessible, and secure, allowing for smooth data exchange.

Offensive operations through OCO can be used to map adversary networks, pinpoint critical targets, and plan cyberattacks to achieve effects against their capabilities, which will result in an operational advantage.

Intelligence operations through CyISR can involve mapping the cyberspace terrain of red cyberspace and collecting intelligence on adversaries' cyber capabilities, vulnerabilities, and intentions. It includes passive monitoring, active reconnaissance, and data analysis to understand adversary cyber behaviour. This intelligence supports the planning of DCO, OCO and other military operations.

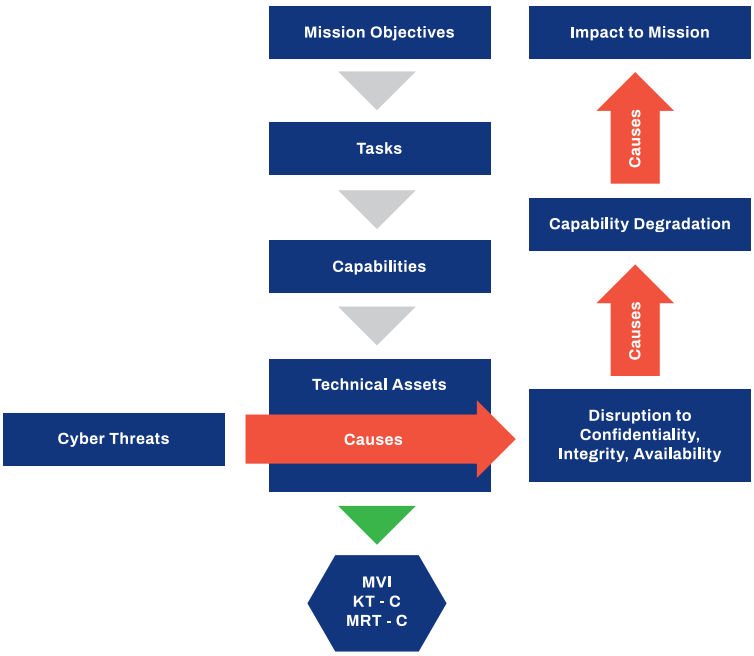
3.8 CYBERSPACE TERRAIN ANALYSIS MODEL

Two models that aid in identifying key terrain cyber and visualising cyberspace terrain in relation to the mission are the modified Mitre Crown Jewels analysis (Figure 3-7)

44 (NATO Standardization Office, 2025)

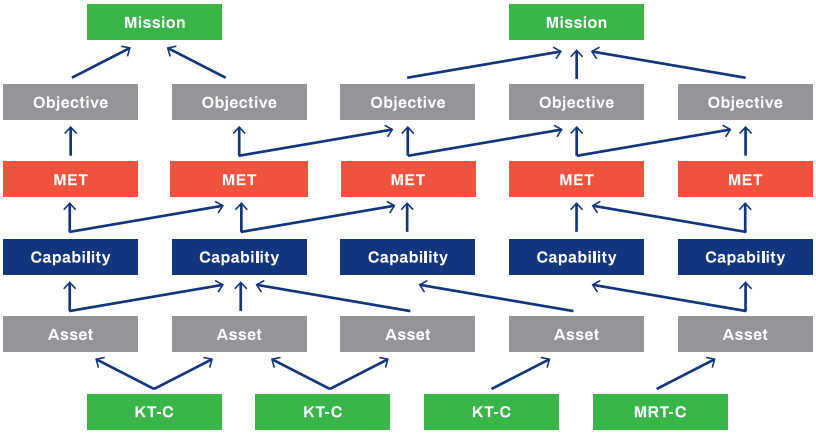
and the Cyber Mission Stack (Figure 3-8).[45] Both models describe cyberspace from the perspective of mission objectives, mission essential tasks (MET), capabilities, and technical assets. This breakdown allows for the identification of essential assets, key terrain cyber, and the establishment of interdependencies. The modified Mitre Crown Jewels model takes it a step further by assessing the impact that the loss or reduced functionality of these systems would have on the mission.

FIGURE 3-7: A MODEL TO IDENTIFY KEY TERRAIN CYBER USING THE MITRE CROWN JEWELS ANALYSIS PROCESS MODIFIED



45 (Colonel (Ret.) Jeffrey A. Voice, 2022).

FIGURE 3-8: A MODEL TO IDENTIFY KEY TERRAIN CYBER USING THE CYBER MISSION STACK



3.9 CYBER COMMON OPERATIONAL PICTURE (CYBER COP)

The cyber common operational picture, referred to as the recognised cyber picture by NATO Allied Command Transformation (ACT).[46]

As a centralised point for information, it enables coordination and collaboration in response to the evolving cyberspace situation. It provides commanders' and decision makers with the current state of cyberspace and cyberspace operations in the areas of interest and areas of responsibility, which is relevant for mission success. Among other things, it displays the current state of assigned cyberspace and the impact of cyber threats. It considers strategic, operational, and tactical levels so that the commander has true cyberspace situational awareness. It includes information from all CIS systems and data from cyberspace operational activities and their implications at the strategic, operational and tactical levels.

In order to achieve situational awareness in cyberspace, we require a number of things:

- Missions: The cyber command must understand the cyberspace zones[47] and how they are linked to the other operational domains. Where are we operating? When are the most important times of those operations? What are the critical information exchange requirements upon which decision

46 ACT uses the term recognised cyber picture so as to use the same definition used in planning - cyber common operational picture (CCOP) or to imply that it is only for the operational level

47 See Figure 3-3 (Cyberspace zones).

makers rely? The answers to these questions come from the mission owners, who are also the individuals who can decide whether a risk in cyberspace is acceptable or must be mitigated.

- The cyber command also needs to understand the CIS and technical aspects that directly support and enable all missions across all domains. This requires the breaking down of missions into discrete business processes, an understanding of the data and information that are required by those business processes, and lastly, an understanding of the CIS services, systems, and applications that provide that data and information. When you have that detailed understanding of your CIS, you can understand implications at all levels: data, business process, and ultimately the impact on the mission. When a node goes down, what part of the mission is impacted? Does the mission stop, or is it degraded?
- Intelligence: The cyber command needs to understand the current threat picture. We must understand the active threats against the mission. When potential adversaries are identified, we can access the tactics, techniques, and procedures they use to ensure we are defending against them, thereby enabling cyberspace operations to focus our defensive actions. We obtain this intelligence through intelligence channels, information provided by commercial subscription services, industry service providers, the media, and open sources.
- Data Integration: A Cyber COP integrates and contextualises data from various sources, such as network logs, intrusion detection systems, threat intelligence feeds, security event information, and operations relevant information, to provide a holistic view of the cyberspace environment.
- Visualisation: Visual representation of the cyber common operational picture is crucial for effective decision making. A cyber common operational picture visualises real time situational awareness, allowing organisations to identify and respond to cyber threats.
- Collaboration: Effective and timely information sharing, coordinating response efforts, and aligning strategies are crucial for effective cyber defence. Collaboration among stakeholders, such as cybersecurity teams, IT departments, host nations' governmental entities, and partners, ensures a comprehensive picture of cyberspace.

3.10 CYBERSPACE AND THE TOTAL DEFENCE APPROACH

Due to the complex relationships and dependencies in cyberpace and the interconnected nature of modern society, military organisations rely on many areas that are outside their control. Cyber activities can impact military operations and organisations in

unpredictable ways. Additionally, adversaries may target green or white cyberspace zones to influence the civilian population in support of their strategic objectives.

This situation creates two key requirements for a military cyber command:

- **Communication and coordination:** The cyber command must establish clear lines of communication and coordination with relevant civilian entities, including government agencies, national and multinational corporations, and non governmental organisations.
- **Defence beyond military CIS:** The command must have mechanisms in place to defend cyberspace assets outside military CIS if and when assigned.

Given that the cyberspace domain is contested and military cyber activities occur throughout all phases of conflict, including peacetime, cyber defence must also be continuous. Resilience cannot be built only in response to a crisis but must be developed and tested in peacetime. Therefore, a cyber command should focus on creating policies and mechanisms for a comprehensive, whole-of-society approach to support national resilience throughout all phases.

3.11 CHARACTERISTICS OF CYBERSPACE OPERATIONS

Understanding cyberspace from the perspective of its characteristics will allow staff to consier cyberspace and the possible operational options in an appropriate manner. Some of the characteristics of cyberspace are as follows:

Reach: Cyberspace operates beyond the physical boundaries of other domains. Global connectivity allows actors to create near instantaneous effects anywhere in the world. Cyberspace operations are constrained only by the level of connectivity, not geography. Where a target of interest is not connected through cyberspace, operators from other services such as special operations forces (SOF) can support cyber command to achieve remote connectivity.

Asymmetric: Cyberspace enables small groups or individuals with sufficient resources, motivation, and skills to execute attacks with disproportionate, strategic, or large scale effects.

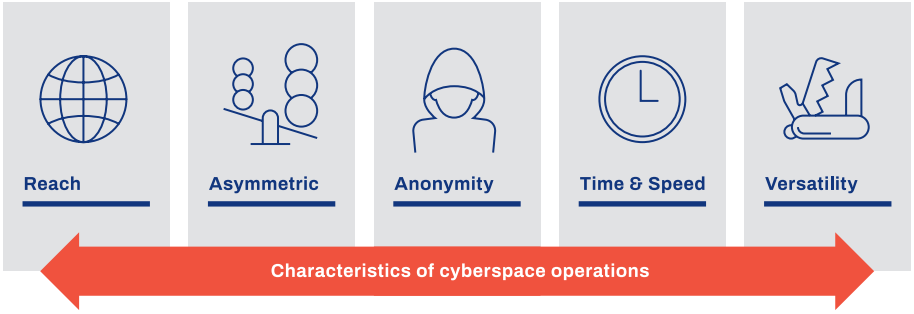
Anonymity: The cyberspace domain allows actors to remain anonymous, disguising their intentions. This anonymity complicates attribution and accountability.

Time and speed: Cyber capabilities vary from simple tools developed quickly to sophisticated systems requiring lengthy preparation. Some cyberspace operations such as DCO can be conducted quickly, given the right conditions. Key time related considerations include the following:

- Actions in cyberspace can produce effects which are immediate or intentionally delayed.
- Preparation time depends on the type of cyberspace operation, supply chain, build time, deployment time, or factors like target complexity, intelligence gathering, and anonymity.

Versatility: Cybers effects can be designed to be temporary, reversible, or irreversible; in some cases, the associated decisions can be adjusted even after deployment. Tools may be reverse-engineered and reused against the originator.

FIGURE 3-9: CHARACTERISTICS OF CYBERSPACE OPERATIONS



3.12 CYBERSPACE OPPORTUNITIES AND CHALLENGES

Opportunities Related to Cyberspace as a Domain

Cyber effects can be generated at multiple locations at the same time or distributed over time. Although it is difficult to fully predict collateral damage (second and third order effects), cyberspace operations may allow for more proportionate effects and improved risk management compared to traditional warfare. Cyber capability development can often remain hidden from early detection. Adversary tactics, techniques, and procedures, once discovered, can be adapted and reused for defensive or offensive purposes. These capabilities may provide an asymmetric advantage, potentially overshadowing the adversary's strengths in other military domains.

Infiltrating an adversary's network and developing an exploit may require significant time and effort. However, once established, cyberspace provides nearly instantaneous global reach, allowing for the simultaneous distribution of force across both space and time.

New and emerging technologies present both opportunities and challenges that need to be monitored and considered by the cyber commander. Artificial intelligence and machine learning can rapidly analyse massive data sets to spot threats and automate security tasks more efficiently. Blockchain technology, with its emphasis on secure data ledgers, enhances data integrity and makes tampering easier to detect.

Cyberspace operations may be carried out on their own or as a part of multi-domain operations. They can both generate valuable effects by themselves and enable activities in other domains.

New and unknown zero day vulnerabilities and opportunities continually arise as the terrain changes. Targets are in motion; no offensive or defensive capability remains effective indefinitely, and no advantage is permanent. 'Well defended cyberspace terrain is attainable but is continuously at risk. Adversary offensive activities persist because opportunity costs are low, and accesses, platforms and payloads can remain useful for extended periods.'[48] Adversaries are constantly researching and improving their tactics, techniques, and procedures in order to exploit new and emerging vulnerabilities.

To oppose threat actors, knowledge sharing and cooperation are esential. Knowledge is crucial to understand technological evolutions, anticipate adversary TTPs, and develop our own defence, intelligence, and offensive capabilities. Cooperation is a real force multiplier and is enabled by sharing knowledge of adversary TTPs and by giving mutual assistance during cyber incidents.

Challenges Related to Cyberspace as a Domain

Preparation time: for cyberspace operations can vary greatly, based on factors such as the maturity of the target, desired effects, target complexity, intelligence gathering needs, anonymisation requirements, and measures to mitigate collateral damage. In CIS Operations (CISOPS) and Defensive cyberspace Operations (DCO), preparation may be influenced by issues such as supply chain constraints, the availability of subject matter experts, or the need to maintain service availability during upgrades. For Offensive Cyberspace Operations (OCO) and cyberspace intelligence, surveillance, and reconnaissance operations (CyISR), it can take weeks, months, or even years to gather intelligence on an adversary's network, develop an exploit, and obtain the necessary authority and approval to execute.

48 (US Cyber Command, 2018).

Human resources: Skilled personnel are a key asset to the cyber command. Recruitment of scarce talent may require adjustment of requirements, with possible consequences for service employment. Skills are highly perishable, and this has an impact on the management of human resources. Constant attention must be given to attracting new talent with the appropriate skills and to educating and retraining existing personnel.

3.13 ATTRIBUTION

Attribution concerns the identification or location of an attacker or attacker's intermediary. This activity is undertaken after an attack has been detected and may be conducted while the attack is in progress or after its conclusion. Defensive cyberspace operations (DCO) will generally prioritise the mitigation of an attack over the establishment of the identities of the parties responsible. Attribution is a prerequisite for planned reciprocal action and should, therefore, precede offensive cyberspace operations (OCO) that are conducted in response to hostile activity.

Attribution has intelligence, technical, legal, and political aspects. The cyber command may be involved directly in any or all of these aspects of attribution. The exact level of involvement depends on the division of responsibilities to each nation. Attribution is heavily dependent on a combination of cyber forensics and cyber threat intelligence. The sources to determine the attribution range from open source intelligence (OSINT) or technical analysis to closed sources and other available intelligence capabilities, such as signals intelligence (SIGINT) and human intelligence (HUMINT). These sources are not limited to national capabilities. Obviously, the combination of a variety of possible sources enhances the degree of certainty concerning the developed hypotheses.

Depending on the situation, particular actors may try to hide their identities and deflect attention to other parties by conducting false flag operations. Therefore, attribution must not rely on technical characteristics alone but needs to be backed up by corroborating evidence from other sources to reach a satisfactory level of certainty. Necessary resources may be derived from capabilities available within the cyber command or the wider defence organisation, as well as public or private sector partners. Cooperation with public sector parties such as government CERT and law enforcement can provide a useful boost to organic capabilities that are available to attribute actions in the cyberspace domain. Private parties may also play a role in the establishment of attribution for cyber incidents and events, either through direct employment by authorities or on their own initiative. While these private parties may provide manpower and specialised skills not available to the military or the public sector, it is important to take into account the particularities associated with this kind

of resource. Private cybersecurity companies may assist in national attribution, but their contributions alone do not constitute national attribution.

It is possible to distinguish between different forms of attribution. Factual attribution refers to a technical assessment and/or other fact based sources of the origin of cyberattack. Legal attribution means the assessment of the cyberattack as a breach of international law. Thus, legal attribution is a national sovereign prerogative implying a purely political decision taken at higher levels than the cyber command. The political nature of legal attribution includes not only the attribution in itself but also the decision to convey, publicly or privately, such a decision and/or the evidence on which it is based. In general, legal attribution should be decided through a case by case assessment on the basis of all relevant facts and circumstances. Nevertheless, in case of legal attribution, no burdens or standards of proof are settled by international law.

As a rule, acts executed by the organs of a state are attributable to the state of their origin. Regardless of the functions of the organ – legislative, executive, judicial, armed forces, or any other its acts are counted as the acts of a state. The conduct of a non-state actor shall be considered the act of a state if it is acting on the instructions of, or under the direction or control of, that state. Non-state actors are considered to be acting under the effective direction or control of a state when they direct or control the specific operation and the conduct complained of is an integral part of that operation.[49] In the case of non-state actors, regardless of effective direction or control, a state may still be held responsible if its territory is used for malicious cyber activities and it has not taken all appropriate measures reasonably available to detect, investigate, and address the situation.

It should be noted that targeted restrictive measures are differentiated from legal attribution of cyberattacks to a third state. The application of targeted restrictive measures, including to a person acting as an organ for a third state, such as in the case of a member of the armed forces (e.g. Council Decision [CFSP] 2020/1127 of 30 July 2020), cannot be considered legal attribution. In case of targeted sanctions, the affected subject might ask for a judicial review of the restrictive measure, in accordance with applicable procedural law. Therefore, although the competent tribunal may show some deference toward the designation, the attribution of targeted sanctions should be characterised by well founded reasons supported by evidence.

3.14 REFERENCE CYBER COMMAND STRUCTURE

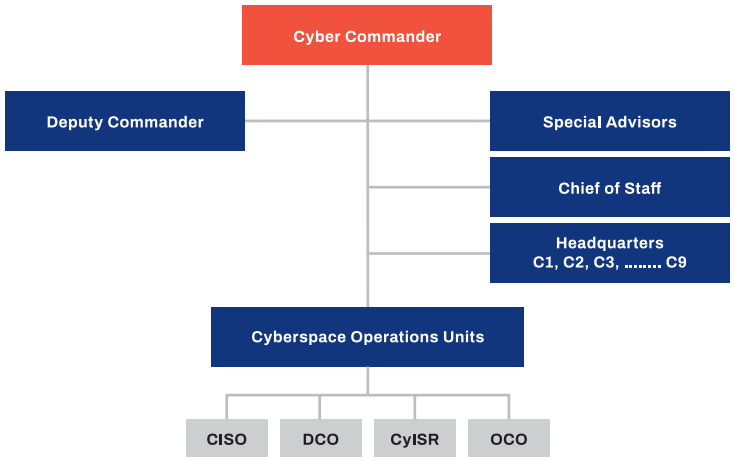
A standalone command structure, branch, or military service dedicated to overseeing cyberspace operations will maximise capabilities, enhance coordination, eliminate

49 This principle is expressed in rule 17 of Tallinn Manual 2.0 [Schmitt, M. (2017)] and mirrors the "effective control" test in the Nicaragua judgment (Nicaragua v. United States of America - Military and Paramilitary Activities in and against Nicaragua - Judgment of 27 June 1986, International Court of Justice)

duplication, and optimise the use of scarce resources. This dedicated entity should direct and control the key categories of cyberspace operations within its area of responsibility: CIS Operations (CISOPS), Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO), and Cyberspace ISR operations (CyISR). The cyber command should be prepared and postured to carry out the full spectrum of cyberspace operations. The cyber command must be structured and staffed in a way that it has the ability to not only support operations in cyberspace as a whole but also to have domain specific knowledge and capability for the land, sea, air and space domains.

To execute cyberspace operations, the cyber command will have 'manoeuvre' elements either as a part of the cyber command or as a subcommand, depending on, among other considerations, size, structure, and responsibilities. Responsibilities and tasks will be described further in Annex C. A reference cyber command is proposed (Figure 3-10). This must be seen as a modular structure that covers the core activities of cyberspace operations:

FIGURE 3-10: REFERENCE CYBER COMMAND STRUCTURE



Functions / Elements which enable Cyberspace Operations *

CIS Infrastructure
Deployable / Tactical CIS
Cybersecurity
Information security
AUDIT
Threat Assessment
INTEL

SOC
CERT
RRT
Threat hunt
Threat Emulation
Cyber Threat Intelligence
Research and Development

Operating systems
Operational Technology
Information assurance
Cyber awareness
Mission assurance

Special Advisors *

POLAD
LEGAD
Public Relations Officer

* Non exhaustive list

3.15 CYBERSPACE MANOEUVRE ELEMENTS

Cyberspace manoeuvre elements are assigned to execute cyberspace operations. This is achieved by deploying cyberspace operations teams into cyberspace areas of operation physically, virtually, or logically in order to achieve the mission objectives. Gaining and maintaining access to the information layer is required to manoeuvre in cyberspace. Cyberspace operations can enable force projection without the need to establish or maintain a permanent physical presence in a location.

Cyberspace operations teams deployed to physical areas of operation can obtain additional support through reach-back facilities to cyber command. Persons and assets assigned to specific roles and functions can be reassigned to support, augment, or enhance the capabilities of a cyberspace operation.

CISOPS

CIS operations teams are responsible for establishing, maintaining, and securing the communications and information systems critical to military operations. For the enterprise or static CIS, they can be located centrally or regionally. Tactical CISOPS teams can be deployed forward to establish or maintain CIS systems in new or existing mission areas. Those teams are assigned to provide, among other things, technical expertise, coding, and infrastructure, such as training elements, a tech department, and cyber ranges.

SOC / NOC / NSOC

A security operations centre (SOC) is a command centre facility for a team of cyber professionals that is organised to detect, analyse, respond to, report on, and prevent cybersecurity incidents in cyberspace. The SOC conducts real time monitoring of network traffic, routers, switches, desktops, servers, endpoint devices, databases, applications, and other systems on a continuous basis, looking for signs of a security incident. A SOC operates around the clock in order to identify, detect and mitigate threats. SOC personnel have the advanced information technology and cybersecurity skills required to monitor, detect and respond to cybersecurity incidents. Cybersecurity incidents that need further attention and/or analysis are escalated to the CERT.

In some cases, a SOC is integrated with the network operations centre (NOC). A NOC is a centralised location where IT professionals monitor, manage, and maintain an organisation's network infrastructure and ensure its optimal performance and availability. In cases where a SOC and NOC are collocated, it can be referred to as a network and security operations centre (NSOC).

CERT / CSIRT

A computer emergency response team (CERT) or a computer security incident response team (CSIRT) is a team of cyber experts organised to analyse, respond to, report on and mitigate cybersecurity incidents. These teams are responsible for detecting, analysing, mitigating, and resolving security threats and incidents in accordance with their mission.

RRT

A rapid reaction team (RRT) is a segment of a CERT that can be deployed quickly. The primary task of the RRT is incident response on a site where remote technical assistance is not an option. The RRT has a short notice to move period, depending on the alert status. It consists of a small team of experts, usually around six persons, who represent the CERT capability. Where an RRT is deployed forward, it has a deployable technical kit. The composition of the team depends on the initial assessment of the assigned cyber incident. To be able to fulfil assigned tasks, a CERT needs to have a highly qualified and experienced team that is trained on a regular basis. An RRT can use the CERT as a reach back facility to expand the RRT resources and capabilities.

DCO

Defensive Cyberspace Operations (DCO) teams are responsible for conducting defensive actions and effects in cyberspace. DCO teams must be established on a permanent basis, ready to be tasked as needed. DCO team may be formed temporarily by reassigning personnel from other units and teams for a specific period and mission. DCO is responsible for threat hunting on its own networks or other networks temporarily within its area of responsibility or area of interest.

OCO

Offensive Cyberspace Operations (OCO) teams are responsible for conducting offensive actions and creating effects in cyberspace. The size and composition of a team will vary depending on the mission and the skills required. OCO teams are highly skilled and should be dedicated teams specifically trained, prepared and postured to conduct offensive cyberspace operations.

CyISR

Cyber Intelligence, Surveillance, and Reconnaissance (CyISR) manoeuvre teams are tasked with gathering, analysing, and disseminating intelligence related to cyber threats and adversary capabilities. These teams can be either permanent, continuously monitoring the cyberspace environment, or assembled for specific intelligence gathering missions. CyISR teams focus on mapping adversary cyberspace, TTPs, and providing actionable intelligence to support cyber commanders' requirements. Intrusive CyISR is carried out by OCO teams according to CyISR requirements.

Liaison Elements

Like all military services and domains, cyber considerations need to be taken into account as early as possible in the planning of operations. Therefore, liaison elements need to be installed and sent to other component commands in order to ensure that cyberspace is reflected in the development of courses of action and scheme of manoeuvre. These liaison elements need to be educated and trained in such a way that they can act as cyberspace experts who can advise the operational commander concerning cyberspace operations. Furthermore, they need to be experts in the process of operational planning and how to incorporate cyberspace operations into the process.

Liaison elements can be sent to other military and governmental entities that are responsible for strategic level planning. In addition, liaison elements can be sent to organisations which have been identified as key terrain cyber but which are not under the command and control of the military.

Staff Integration

Effective staff integration is achieved when functional expertise from across the staff and from external mission partners is brought together in direct support of the commanders' decision. Decision boards leverage the analytical capability of the entire staff and mission partners to support decision requirements through interaction between working groups and operational planning teams for current and future operations.

For example:

- The cyber operational working group supports the mission analysis, course of action (CoA) development, scheme of manoeuvre development, war gaming, etc.
- A cyberspace representative contributes to the operational and strategic effects targeting board.
- Other working groups and boards as required.

3.16 CREATING THE CYBER BATTLESPACE

Creating the Cyber Battlespace refers to the strategic and tactical process of shaping and preparing both physical and virtual environments so that cyberspace operations can be planned and conducted effectively. This involves establishing cyberspace infrastructure, physical buildings, cyber ranges, processes and procedures to ensure effective operational capability and which enable the full spectrum of cyberspace operations and can enable and support all services. Some key components of the cyber battlespace include:

Physical Infrastructure and Operational Centres

This includes secure data centres, IT systems, cybersecurity, and operational buildings designed so that cyberspace operations can be planned, prepared, conducted, and monitored, as well as integrating cyber considerations into wider operational planning. A well structured physical environment fosters cross pollination of skills, enabling cyberspace operations teams to support one another. Additionally, these centres must be designed to accommodate support from external agencies, industry partners, and academia. Furthermore, they must be able to scale up operations rapidly, providing surge capacity when major cyber incidents occur.

Virtual Environments to Conduct Cyberspace operations

The virtual environments, in order to conduct CIS, defensive and offensive cyberspace operations, also need to be considered. These include dedicated server infrastructure, software, secure cloud services, on-premises monitoring and reporting, and secure obfuscated infrastructure, etc.

Cyber Ranges

Cyber ranges are specialised virtual environments designed to simulate cyberattacks, test defences, and train personnel. These dedicated platforms replicate real world IT infrastructures, providing a safe environment for individuals and teams to develop their skills. Organisations can use cyber ranges to improve response times and allow operators to create and refine new tools, tactics, and procedures in a controlled setting without endangering real world systems.

Mobile capability

Mobile capability refers to conducting and supporting cyberspace operations using deployable manoeuvre elements. This includes supporting other operational services and conducting cyberspace operations in locations that cannot be reached remotely. Additionally, it is necessary to establish the appropriate authorisation, technology, processes, and procedures to prepare and posture cyberspace manoeuvre elements to be able to conduct cyberspace operations when required.

4. Cyberspace Operations

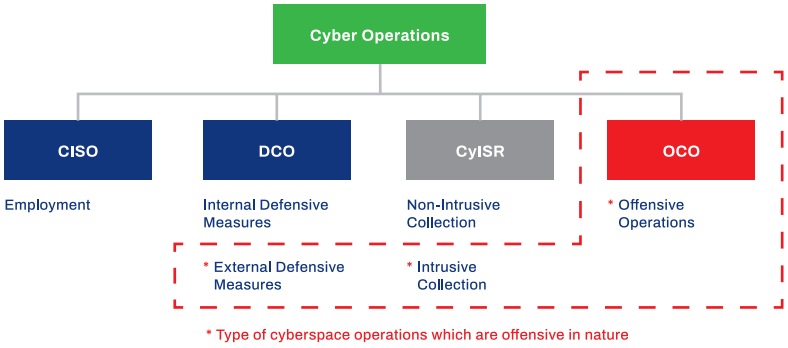
Cyberspace operations are crucial for maintaining a nation's sovereignty during peacetime, ensuring freedom of movement (FoM) within its area of interest (AoI) in cyberspace and contributing to achieving military objectives. Cyberspace operations can be either the main effort or supporting effort, synchronised with joint and or multi-domain operations involving land, sea, air, space, and special operations. These operations must be aligned with political and military objectives. The interconnectivity and interdependence of cyberspace increases the risk of unintended and cascading first, second, and third order effects in the physical, virtual, and cognitive effect dimensions.[50]

The cyber command is responsible for planning, preparing, coordinating, deconflicting, and conducting full spectrum cyberspace operations. Cyberspace operations are categorised based on the intent or objective required. In the cyberspace domain, there are four types of cyberspace operations as follows.

- **Communication and Information Systems Operations (CISOPS):** Actions taken to employ, secure, operate, and maintain CIS in a way that creates and preserves confidentiality, integrity, and availability (CIA), as well as user authentication and non-repudiation.[51]
- **Defensive Cyberspace Operations (DCO):** Actions in or through cyberspace to preserve own and friendly freedom of action in cyberspace.[52]
- **Cyberspace Intelligence, Surveillance, and Reconnaissance Operations (CyISR):** The activities and capabilities within or through cyberspace domain to collect data and information in order to achieve results that contribute to intelligence.[53]
- **Offensive Cyberspace Operations (OCO):** Actions in or through cyberspace that create effects to achieve military objectives.[54]

50 First-, second-, and third-order effects will be described further in Chapter 5.
51 (NATO AJP 3.20 Study draft 1, Mar 2025)
52 (NATO Standardization Office, 2025)
53 (NATO Standardization Office, 2025)
54 (NATO Standardization Office, 2025)

FIGURE 4-1: CYBERSPACE OPERATIONS FRAMEWORK



4.1 CHARACTERISTICS OF EFFECTIVE CYBERSPACE OPERATIONS

Cyberspace operations are critical to achieving mission success. Cyberspace operations must be coordinated and conducted according to wider mission requirements. The following is a non exhaustive list of principles that can be relevant when planning and conducting cyberspace operations:

- Have an operational and mission mindset.
- Be for a defined time and purpose.
- Have focused actions and effects.
- Be intelligence driven for a specific threat.
- Support the mission and/or the cyber commanders' objectives.
- Maintain unity of effort.
- Have clear authorities and an approval process.
- Have clear command and control; coordinate with all relevant internal cyberspace actors, such as CIS operations teams and operational planning boards, as well as external actors as required.
- Coordinate with civilian authorities and industry as required.
- Have legal agreements and a memorandum of understanding in place, with clearly identified roles, responsibilities, and points of contact with organisations and entities outside your control (identified as KT-C in the CPAL).
- Follow national and international law and the specific mission legal framework.
- Be precise, proportional, and necessary.
- Be coordinated and deconflicted with operational and strategic effects targeting boards.

4.2 COMMUNICATION AND INFORMATION SYSTEMS OPERATIONS (CISOPS)

CIS operations can be defined as: 'actions taken to employ, secure, operate and maintain CIS in a way that creates and preserves confidentiality, integrity, and availability (CIA), as well as user authentication and non-repudiation'.

CIS operations occur in blue or assigned grey cyberspace, in static permanent locations and/or deployable temporary locations. They can include the deployment and integration of systems from multiple internal and external stakeholders. They are an ongoing process in order to configure, secure, monitor, operate, extend, maintain, and sustain CIS infrastructure and services which ensure confidentiality, integrity, and availability (CIA). CISOPS manoeuvre elements can be deployed forward with the ability to access reach back support when needed.

CIS operations should factor in several perspectives which need to be balanced for a holistic approach, including:

- **Operational needs:** The primary purpose of the terrain and will dictate functions and services necessary to support the mission.
- **Cybersecurity:** The practice of reducing risk and protecting communication and information systems (CIS) from cyber threats while ensuring resilience and conducting audits.
- **Defensibility:** The ability of a given area of blue terrain to facilitate defensive actions.

Operational Needs

When CIS networks are designed, built, maintained, and sustained, they must be tailored to be usable and support the requirements of the mission. Sustainment involves an organisation's ability to maintain its essential functions, quickly recover from incidents, and guarantee operational capabilities in all circumstances.

Cybersecurity

Cybersecurity can be defined as: 'the application of security measures for the protection of communication, information and other electronic systems, as well as the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication, and non-repudiation'.[55]

These activities occur as part of CISOPS on a daily basis. The correct application of cybersecurity is the foundation for cyber defence.

55 (NATO Standardization Office, 2025)

When designing, building, and maintaining CIS networks, adopting a layered security by design approach is essential. This approach starts with an 'assume breach' mentality, where the potential for intrusions is considered and mitigation measures incorporated from the outset. A network must have multiple layers of security to avoid single points of failure, ensuring that if one layer is compromised, others remain intact to protect the network.

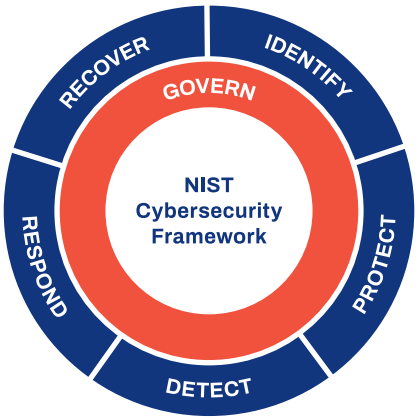
Cybersecurity mitigates and reduces but does not eliminate the risk of a cyberattack. It is the practice of protecting systems and data from a broad range of threats and vulnerabilities, unauthorised access, and damage. This is achieved through a holistic approach that applies many principles, such as but not limited to information security, application security, endpoint security, identity and access management, cloud security, risk management, and compliance.

Among other activities, CISOPS must build to a zero-trust approach, conduct cybersecurity audits and vulnerability assessments, and apply cybersecurity frameworks such as the National Institute for Standards and Technology (NIST) cybersecurity framework (CSF) 2.0.

- **Zero trust:** Continuously verifying the identity and integrity of every user and device, ensuring that only legitimate users can access resources. This constant verification reduces or disrupts entry points for attackers, making it significantly harder for them to infiltrate or traverse the network.[56]
- **Audit:** A cybersecurity audit team verifies that security measures are implemented and maintained in accordance with national cybersecurity policies and directives. The audit team is also responsible for:
    - Providing advice and guidance on cybersecurity policies and directives
    - Reviewing and approving cybersecurity related documentation, e.g. standing operating procedures (SOPs), security accreditation plans, and risk management reports
    - Providing a statement of security accreditation for the CIS
- **Vulnerability assessment (VA):** A vulnerability assessment team performs:
    - A security test and evaluation (ST&E) to ensure that the configuration is established and maintained in its approved state through vulnerability scans and assessments.
- **Cybersecurity framework:** Organisations should follow a recognised best practice security framework. There are many frameworks, such as the internationally recognised National Institute of Standards and Technology (NIST) cyber security framework (CSF) 2.0 (Figure 4-2).

56 (ASD, 2025)

FIGURE 4-2: NATIONAL INSTITUTE STANDARDS AND TECHNOLOGY (NIST) CYBER SECURITY FRAMEWORK 2



The CSF 2 is applicable to all industries and organisations. It describes the following functions:

- **Govern:** Establish and monitor the organisation's cybersecurity risk management strategy, expectations, and policy.
- **Identify:** Help determine the current cybersecurity risk to the organisation.
- **Protect:** Use safeguards to prevent or reduce cybersecurity risk.
- **Detect:** Find and analyse possible cyberattacks and compromises.
- **Respond:** Take action regarding a detected cybersecurity incident.
- **Recover:** Restore assets and operations that were impacted by a cyberattack.

Defensibility

Defensibility is the capability to effectively defend an assigned area of cyberspace. Defenders must assume the architecture will never fully be secure and incorporate a focus on building a defensible architecture.[57] This involves both technical and procedural elements.[58]

- **Technical:** These include creating a comprehensive asset inventory, setting up secure access points for cyberspace operations, creating zones, deploying sensors and tools, and configuring systems to enhance defence capabilities.
- **Procedural:** These include comprehensive planning for cyberspace operations, establishing routines for coordination and conflict resolution, and maintaining a clear situational awareness of the cyberspace environment.

57 (Dr_Jacob_Benjamin, 2023)
58 (Gunnvall Ekstorm, 2022)

Some of the measures that affect defensibility are also important for security and/or operational needs. Others might be counter to the requirements of the other perspectives, such as the need to be able to break encryption at given points or alter configurations dynamically.

CISOPS Skills and Functions

There are many skills and functions that enable CIS operations. Units and sections should be enabled and empowered to carry out the necessary tasks. A non-exhaustive list of skills and functions appears below.

- IT operations
- Network operations
- Application specialists
- Infrastructure specialists
- Database specialists
- Cybersecurity
- Tactical cyber threat intelligence
- Information security
- Security operation centre / network operations centre (NSOC)
- Deployable CIS
- Tactical CIS networks
- Tactical radios

4.3 DEFENSIVE CYBERSPACE OPERATIONS (DCO)

Defensive cyberspace operations can be defined as: 'actions in or through cyberspace to preserve friendly freedom of action in cyberspace'.[59]

The purpose of DCO is to prevent, mitigate, or respond to incidents, threats, and adversary cyberspace operations in order to ensure freedom of movement (FoM) in assigned cyberspace. This can be achieved through a combination of proactive and reactive measures, such as continuous network monitoring and advanced analytics. A key tenet of a DCO is to use deception to mislead or deceive an adversary through the deployment of techniques such as honeypots or honeynets[60] designed to attract adversaries to analyse their tactics, techniques and procedures.

DCOs can be used to defend cyberspace identified as key terrain cyber (KT-C) during the cyberspace terrain analysis process. DCOs are planned activities with specific objectives and carried out for a defined period of time. They can occur in blue, green, and white cyberspace.

59 (NATO Standardization Office, 2025)
60 A honeypot is a strategy that involves setting up a decoy system to attract cyberspace threat actors diverting them from real assets and gathering intelligence on their TTPs

Transition to DCO

The aim of cybersecurity is to secure assigned cyberspace from a general, overall threat, whereas DCO's intent is to defend against specific threats in assigned cyberspace. Therefore, the transition to DCO occurs when a threat is identified, perceived or to confirm that no threat exists which could impact the mission. At this point, the cyber commander decides to implement defensive actions, including, but not limited to:

- Observing adversary tactics, techniques, and procedures (TTPs)
- Halting the adversary's advance
- Deploy deception
- Defending critical assets and information systems
- Hunting for adversary activity and advanced persistent threats (APT)
- Defending, maintaining, or regaining control of KT-C.
- Maintaining freedom of movement in assigned cyberspace.
- Mapping assigned cyberspace to aid DCO activities
- Potentially creating the conditions for a counterattack[61]

DCOs can be conducted in an area of interest (AoI) or avenue of approach (AoA). They may be concentrated on a system or specific information. Similarly, a DCO can be conducted in a node or link connecting different cyberspace sections.

DCO can be further categorised as internal and external defensive measures.

- **DCO internal defensive measures (DCO – IDM):** Conducted in assigned cyberspace, or KT-C. They can include active and passive measures to identify, mitigate, and defeat adversary activity.
- **DCO external defensive measures (DCO–EDM):** These are actions taken outside assigned and defended cyberspace in order to mitigate active or imminent cyberattacks or create the conditions for a counterattack. The intent and purpose of DCO – EDM is to halt adversary actions when doing so cannot be achieved through internal defensive measures. DCO–EDM is similar to OCO and should be conducted with similar authorities and approvals and in accordance with national and international law.

Dedicated DCO teams must be established, prepared and postured to defend assigned cyberspace. Additional DCO teams can be assembled as required. The skills required to form a DCO team include similar skills to CISOPS, but specific skills can be different depending on the mission and the systems that need to be defended. A team conducting DCO can be deployed forward into the physical area of operations (AoO) or be conducted remotely. A team deployed forward may require additional remote support through reach back facility.

61 (Allen, 2020)

Threat hunting is a proactive DCO approach to identifying previously unknown or ongoing threats within assigned cyberspace. Sometimes referred to as 'Hunt Forward' DCO teams can be deployed forward in key terrain cyber to conduct a threat hunt. Threat hunting aims to identify, detect and mitigate cyber threats before they can cause significant damage or affect the mission.[62]

DCO Skills and Functions

There are many skills and functions that enable defensive cyberspace operations. Teams and sections should be enabled and empowered to carry out the necessary tasks quickly and effectively. A non exhaustive list of skills and functions appears below.[63]

- Network mapping
- Vulnerability mapping
- Data analysis and log interpretation
- Cyber threat intelligence analysis
- Threat hunting
- Risk assessment
- Digital forensics
- IT and network systems
- Network and endpoint security

4.4 CYBERSPACE INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE OPERATIONS (CYISR)

Cyberspace ISR operations are defined as: 'the activities and capabilities within or through cyberspace domain to collect data and information in order to achieve results that contribute to intelligence'.[64]

CyISR operations are focused on gathering tactical and operational information required for military planning. It includes but is not limited to the targeting process, information on adversaries' capabilities and intent, and the operational environment. They can act to inform operations within other domains and contribute to the intelligence process, providing the commander with situational awareness. Non-intrusive CyISR can be conducted quickly. Intrusive CyISR operations are intelligence driven and conducted by cyber command and may require substantial preparation times.

The dynamic nature of cyberspace makes ISR within this domain a challenging and specialist task where, in addition to the technical complexity, operations are constrained by strict policy and legal guidelines.

62 (Beecroft & Gilmore, 2023)
63 (Arik, Venables, & Ottis, 2024).
64 (NATO Standardization Office, 2025)

The primary functions of CyISR are to:

- Develop knowledge and understanding: Cyber threat intelligence (CTI) builds a contextual understanding of the environment and actors, analysing their intent, capabilities, and motivations.
- Produce predictive assessments: By reviewing past and current activities, CyISR can reveal potential future actions.
- Assess threat levels: CyISR evaluates threats by analysing three key factors:
    - **Intent:** Understanding the adversary's motivations and reasoning behind potential actions, whether stated or implied.
    - **Capability:** Analysing the adversary's strengths; tactics, techniques, and procedures (TTP); and their ability to maintain and deploy them.
    - **Opportunity:** Assessing the conditions that could allow an adversary to act.
- Intelligence and operational support to CO planning
- Operational commanders' have key roles and responsibilities in CyISR. They provide planning guidance and define the area of interest (AoI), priority intelligence requirements (PIR), and commanders' critical information requirements (CCIR).

CyISR can be categorised as follows:

- **Intelligence** collection disciplines and concepts applicable to CyISR include, but are not limited to:
    - **Open source intelligence (OSINT):** Derived from publicly available information in cyberspace.
    - **Signals intelligence (SIGINT):** The collection and analysis of electromagnetic signals for actionable insights.
    - **Cyber threat intelligence (CTI):**[65] CTI is a civilian concept which can be used in a military environment. It is cyberspace information about existing and potential cyber threats, attack vectors, and the methods and intentions of adversarial cyberspace threat actors. It can be used by CISOPS teams for cybersecurity and cyberspace manoeuvre elements during cyberspace operations. It can also be used by intelligence and the cyber operational working group to inform operational planning.
        - **Strategic level:** Focuses on long term threats that may impact national security, critical infrastructure, and the overall stability of a nation. CTI can be used to provide

65 CTI is a civilian concept and is not a recognised intelligence discipline as understood in a military context.

high level insights into adversarial groups, geopolitical risks, and significant trends in cyber activities.

        - **Operational level:** Focuses on threats that could disrupt or impact specific missions. It includes information on cyberspace threat actor's tactics, techniques, and procedures (TTPs) and their motivations that could affect military or organisational objectives.
        - **Tactical level:** Focuses on the technical aspects of cybersecurity threats, providing detailed information on threats to specific technical systems and networks. It includes information on indicators of compromise (IOCs) that can signify malicious activities.
- **Cyberspace surveillance:** The systematic observation across all domains, places, persons, or objects by visual, electronic, photographic, or other means. Within the cyberspace domain surveillance is the continuous and systematic monitoring of the environment. It is passive and continuous, focused on long term observation to identify things such as patterns, devices and cyberspace actors. Cyberspace surveillance can be achieved through activities such as network scanning and intrusion detection.
- **Cyberspace reconnaissance:** Defined as a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an adversary or to obtain data concerning the characteristics of a particular area. Reconnaissance can be considered as active measures and must be focused in time and space to answer specific requirements. For example, within the cyberspace domain, it can be used during an OCO in red cyberspace to identify adversary physical resources or cyber defences.

CyISR can occur internally in assigned cyberspace or external to assigned cyberspace:

- **Internal:** When conducted within friendly systems or in/through blue cyberspace, in order to identify hostile activities and capabilities.
- **External:** When conducted through cyberspace to gather data from an identified target or adversary information systems or networks.
    - **Non intrusive collection (passive):** When conducted using publicly available pieces of information, for example, using open source intelligence (OSINT) without actively interacting with the adversary.
    - **Intrusive collection (active):** Actively interacting with adversary cyberspace in order to gather information related to the adversary. Active CyISR includes, but is not limited to, system compromise,

data exfiltration, and target observation in cyberspace. Intrusive CyISR can often require significant time to prepare and to get into position. Intrusive CyISR is similar to OCO. It should be conducted with similar processes, authorities and approvals and be carried out in accordance with national and international law.

4.5 OFFENSIVE CYBERSPACE OPERATIONS (OCO)

Offensive Cyberspace Operations (OCO) can be defined as: 'actions in or through cyberspace that create effects to achieve military objectives'.[66]

OCOs aim to create effects in and through cyberspace to achieve military objectives. These operations are conducted in grey and red cyberspace against authorised targets, aiming to establish decisive conditions that support strategic and operational objectives against adversary key terrain cyber.

OCOs can be the main effort (ME) or a supported effort (SE) or be part of joint or multi-domain operations. They require specialised knowledge and experience and are typically authorised at the strategic and political levels. Therefore, a robust authorities and approvals process is required. OCOs are heavily driven by intelligence and can take weeks, months, or years to gather information on an adversary's network, develop an exploit, and move into position. Once in position and authorised, they can be executed in seconds from anywhere. Cyberspace planners must consider the possibility of cascading and unintended effects.

When conducting an OCO, it is vital to ensure careful planning, coordination, and deconfliction with other operations. Moreover, rules of engagement (RoE) and measurable objectives must be defined. OCOs can be used to inflict, effects against adversary targets. The chosen effects must be necessary and proportional. When used appropriately, OCOs can de-escalate a conflict. It is impossible to take full and permanent control or possession of key terrain cyber or completely deny adversaries its use in cyberspace. However, it is possible to temporarily deny adversaries this capability by disrupting or degrading their freedom of action in cyberspace.

When authorised, OCOs can target adversary cyberspace, which can create effects in the physical, virtual, or cognitive dimensions. These effects may include, but are not limited to, disrupting, denying, degrading, destroying, or manipulating adversary

- Command and control systems
- Weapons systems
- Information systems

66 (NATO Standardization Office, 2025)

- Supply chains
- Key terrain cyber (KT-C) as identified in the planning phase.

Before executing OCO, the following points should be considered:

- The cyber weapons used can be stolen, copied, and reused against their creator.
- The use of offensive cyberspace operations may escalate the conflict.
- OCOs are, by their nature, classified operations.
- Actions in cyberspace conducted by third parties can impact planned cyberspace operations.

OCO Skills and Functions

It is essential to map the essential skills and functions required to carry out offensive cyberspace operations. Teams should be prepared, postured, and enabled to carry out the necessary tasks. A non exhaustive list of skills and functions appears below.[67]

- Exploit development
- Client side operating systems and applications
- Networks
- Web application
- Cloud systems
- Evasion techniques
- Operational technology
- Vulnerability mapping
- Risk assessment
- Digital forensics

4.6 SOVEREIGN CYBER EFFECTS PROVIDED VOLUNTARILY BY ALLIES (SCEPVA)

As an organisation, NATO does not intend to develop any offensive cyber capability of its own. Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) is a NATO mechanism used in approved NATO allied operations and missions. During an allied operation or mission (AOM), the SCEPVA process can be used to request offensive cyber effects from participating nations.

The Alliance will benefit from cyber effects provided by nations in accordance with the legal and political principles agreed by the North Atlantic Council (NAC), which abide by AOM dedicated rules of engagement. NATO will not directly task the nation's offensive cyber capabilities. NATO's Cyberspace Operations Centre

67 (Arik, Venables, & Ottis, 2024).

(CyOC) in the Supreme Headquarters Allied Powers Europe (SHAPE) will facilitate the integration of SCEPVA into the military planning process. It will provide willing nations with military objectives to achieve and provide to the NATO operational chain of command the expertise to approve and synchronise the provided effect.

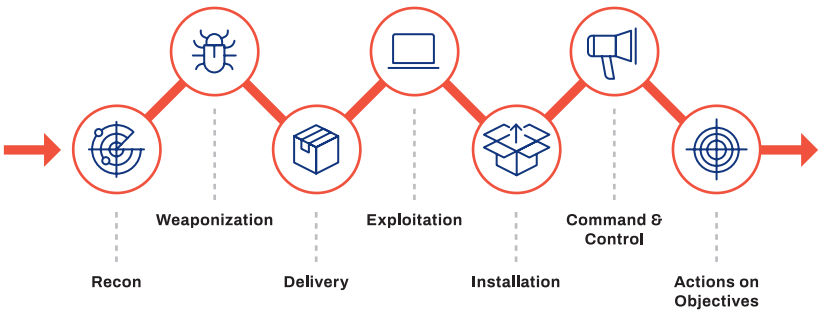
The following points are relevant when requesting the SCEPVA mechanism:

- SCEPVA is provided on a sovereign and voluntary basis by individual Alliance member nations.
- OCO effects must always be considered part of a joint effects function within strategic, operational, and tactical planning processes.
- The NATO Cyberspace Operations Centre (CyOC) is the single point of contact for SCEPVA.

4.7 PHASES OF A CYBERSPACE OPERATION

Like activities in other domains, cyberspace operations can be broken into phases. By doing so, planners can align resources, capabilities, and objectives with the overall mission intent. For cyberspace operations planning at the tactical level, the Mitre Attack Framework is widely adopted. At the operational level, a common approach is to use the Lockheed Martin Cyber Kill Chain, which will be the focus of this publication. This framework can be used for both DCO and OCO planning. The cyber kill chain has seven phases and in practice does not always follow a linear progression. Thus, you may arrive at a point in your operation and may need to move to a previous step, repeat a step, or otherwise take steps out of order. The duration of each phase may also vary. Describing the operation in phases supports the development of the concept of operations and the scheme of manoeuvre.

FIGURE 4-3: THE CYBERATTACK KILL CHAIN[68]



68 (Flaborea, 2024)

- **Reconnaissance:** Information about the target is gathered to identify vulnerabilities, potential entry points, and weaknesses.
- **Weaponisation:** An exploit is developed that will create the desired effect against the vulnerability identified during reconnaissance.
- **Delivery:** The adversary delivers the weaponised payload to the target system using different attack vectors.
- **Exploitation:** Once the payload is delivered, the adversary gains access to the target system by exploiting the vulnerability contained in the payload.
- **Installation:** A foothold is established in the target system and persistence is maintained.
- **Command and control:** The adversary establishes a communication channel to facilitate the transmission of commands and receive data.
- **Actions on objectives:** Action is taken to create the required effects.

By understanding the cyberattack kill chain, defenders can take countermeasures at each stage through the correct employment of people, process, and technology.

4.8 LEGAL CONSIDERATIONS RELATED TO DIFFERENT OPERATIONS

Legal Basis

The deployment of cyber elements, activities, or tools as (military) instruments outside national borders is governed not only by international law but also by domestic law.[69]

One of the basic principles of international law, as also recognised in national policy and doctrine, is that nations may not operate in another state without that state's consent or without a legal basis under international law. Three legal principles reflect this prohibition: the non-intervention principle, the principle of sovereignty, and the prohibition on the use or threat of the use of force in international relations (as expressed in the UN Charter). The legal basis for operating across other state borders is in the UN Charter Chapter 7, (collective) self-defence (Article 51), or authorisation from the Security Council (Article 42).

The prerequisite to use force in self-defence is an armed attack.[70] Other international wrongful acts do not typically give grounds for the use of force. When an international wrongful act against a state stays below the threshold of armed attack but is attributable

69 Military forces still have to adhere to their national laws even when deployed abroad. See J. Stinissen et al., *A Study for Existing and Possible Rules of Engagement* (NATO Cooperative Cyber Defence Centre of Excellence, 2015), p. 15.

70 In order to amount to an 'attack', an operation (regardless of whether it is offensive or defensive) must conclude in violent consequences resulting in injury or death to persons or damage to or destruction of objects. See Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 49(1); and M. Schmitt (2017), Rule 92.

to another state, the victim state has several types of response options. These include but are not limited to, retortive measures, countermeasures, or the plea of necessity:

- **Retortive measures:** They are typically unfriendly but still lawful actions that can be taken against the offending state, often in the realm of diplomacy.
- **Countermeasures:** This is a more formal option that can be used if the conditions[71] for countermeasures are met. Countermeasures are acts that are otherwise unlawful but can be taken by the injured state as a response to a breach of an international obligation. The implementation of countermeasures differs from state to state based on their interpretation of countermeasures.
- **Plea of necessity:** The plea of necessity precludes the wrongfulness of a possible action when certain conditions are met. These conditions include the existence of grave and imminent peril to the state's essential interest, the absence of alternative ways to address the situation, and the determination that the state's need to act to protect itself is more important than the state's compliance with international obligations. Importantly, the plea of necessity does not depend on a prior breach by another state, meaning attribution is not a prerequisite (however, in practice, you would still need to know where the wrongful act originates from, to the extent that that information enables you to stop it).[72]

Further information on these and other legal concepts can be found in the CCDOE cyber law interactive toolkit.[73]

Law Governing Operations

The legal framework that applies during deployment outside a country may differ for each operation, and even sometimes for different areas or phases of the same operation.

International humanitarian law (IHL), or *jus in bello*, is the law that governs the way in which warfare is conducted, including cyberspace operations. This body of law is established, among other things, by the Geneva Conventions I–IV and their Additional Protocols. IHL includes rules for the methods and means of warfare, as well as provisions for the protection of non combatants and civilian objects and property. IHL only applies officially in situations of 'armed conflict'; whether a situation is one of armed conflict depends on a factual evaluation. It is good policy to apply the protective provisions of IHL as a safety margin for all military operations.

71 See also the now customary law: 'Draft Articles on Responsibility of States for Internationally Wrongful Acts', *United Nations Yearbook of the International Law Commission*, 2001, vol. 2, Part 2.

72 (Schmitt, 2017).

73 (NATO Cooperative Cyber Defence Centre of Excellence, 2025)

When conducting cyberspace operations, assessing proportionality and incidental harm to civilian cyberspace infrastructure is much more difficult than with traditional kinetic activities. This challenge also applies to identifying legitimate military targets, or objects that have both military and civilian uses.

Targeting

In the targeting process, it is mandatory to apply IHL. The overall rule for targeting is that it is forbidden to conduct cyberspace operations that amount to an attack against civilians or civilian objects.[74] Even though cyber infrastructure often serves both military and civilian purposes, it can still be targeted in compliance with IHL, provided that there is careful consideration of factors such as civilian components, incidental damage, proportionality, and whether the actions offer a clear military advantage.[75]

In cyber activities, non-state actors may be involved more often than in kinetic activities. This may raise the question of whether these actors can be targeted. If their activities amount to the criteria of the threshold of harm, direct causation, and belligerent nexus, they can be considered to be participating in hostilities and, therefore, can be seen as possible targets.[76]

Rules of Engagement

Rules of engagement (RoE) are mission specific rules for commanders' of military operations that establish the parameters and mandates concerning the use of force or actions that may be construed as provocative towards other parties in the area of operations. Therefore, the RoE are relevant for DCO – EDM, CyISR (intrusive collection), and OCO.[77] RoE are dependent on the mandate[78] or legal basis for the operation in question, often typical in (multinational) missions abroad.. It is specifically important to include cyber capabilities in the planning when preparing the mandate and the RoE for an operation.[79] RoE are not typical in self-defence scenarios.

In a multinational deployment, RoE are drafted and promulgated by the relevant command authorities of the international alliance or union, or – in the case of an operation by a coalition of states in consultation with the states that are participating in

74 Additional Protocol I, Article 48.

75 (J. Stinissen et al.)

76 Ibid., p. 15. See also N. Melzer, *ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (2009), p. 46.

77 RoE for cyberspace are directives to military forces that define the circumstances, conditions, degree, and manner in which force, or actions that might be construed as provocative, may be applied in or by the use of cyberspace. It is elementary that a state can defend its own systems. Therefore, operations that are merely defensive do not need RoE.

78 The legal basis for the operation in combination with the political directives and goals to be adhered to, and attained by, the force commander.

79 Commanders' may restrict the relevant RoE for subordinate commanders' at any time, but they cannot expand them. RoE never restrict the universal right to personal self-defence, provided that the principles of proportionality (no more force may be used than is necessary to counter the threat) and necessity (force should be the last reasonable resort and be absolutely necessary under the circumstances) are adhered to.

the coalition. Based on national policy or national law, a state may impose restrictions on the agreed RoE and issue such restrictions to the deployed forces as supplementary instructions.

Other Legal Considerations

This publication cannot cover all legal considerations, but cyber commanders' must be aware of and seek legal advice on several key areas during cyberspace operations. These include issues related to artificial intelligence, cloud services, digital service providers (DSPs), the private sector, and memorandums of understanding when interacting with and supporting other agencies.

5. Cyberspace Operations Planning

Preparations for all types of cyberspace operations begin in peacetime and continue from crises through to conflict and war. The cyberspace environment is persistently engaged; therefore, the cyber command must continuously update its understanding of the operational environment and adapt plans and operations accordingly. Cyberspace operations can be the main effort (ME) or a supported effort (SE) or be part of joint or multi-domain operations or switch from one to the other. During the planning of cyberspace operations, the cyber command must coordinate, synchronise, and deconflict with other commands and branches.

5.1 POLITICAL, STRATEGIC, AND OPERATIONAL PREREQUISITES

Political and Strategic

For cyberspace operations in areas that fall outside the authority of the cyber command, it is necessary to obtain political guidance and military directives. Political guidance establishes acceptable levels of risk and impact, while military directives convert this guidance into specific mission objectives, scope, and legal parameters. Using this information, potential cyberspace areas of interest are identified and an understanding of the operational environment, along with situational awareness, is developed. From this, the cyber commanders' course of action can be defined.

Operational

Whether it is a CISOPS, DCO, OCO, or CyISR, the type of cyberspace operation, along with its actions and objectives, determines the required levels of access, tools, equipment and expertise. For instance, CIS operations prioritise secure, resilient, and uninterrupted communications in the selection of equipment, tools, and methods. Similarly, DCO, which focuses on preventing, identifying, detecting, and responding to threats, will dictate the technology, hardware, and specialised knowledge required for success. OCO requires an understanding of the adversary's key cyberspace terrain, including their systems, functionality, and specific vulnerabilities. These operations may involve using custom built tools or off the shelf tools to generate the required cyber effects against the adversary's cyberspace assets.

Operational and technical prerequisites may significantly affect the timelines of planning due to the research required or the combined effects of procuring, designing, deploying, and developing new systems, tools, or capabilities.

5.2 CYBER CONSIDERATIONS AND OPERATIONAL PLANNING

The NATO Comprehensive Operational Planning Directive (COPD) is an international standard tool for operational planning and can be applied to the cyberspace domain. Following a planning process such as the COPD supports the commanders' decision-making process. Cyber considerations must be taken into account as early as possible in the planning cycle, whether it is a cyber, joint, or multi-domain operation. The cyber commander must request that cyberspace areas of interest and details of the applicable legal frameworks be identified. Furthermore, the cyber commander must seek coordination, synchronisation, and deconfliction throughout.

The cyber operational working group (COWG) is formed to support the cyberspace planning process. It is a multi disciplinary group from all directorates and staff functions. The cyber operational working group supports the development of the required planning products, ensuring cyber is considered from all points of view. It will contribute to developing the concept of operations (CONOPS), the operational plan (OPLAN).

During the planning process, the cyber commander and staff should consider things such as, but not limited to:

- Full integration of cyber capabilities
- Identifying and countering adversary action in cyberspace
- Identifying and prioritise mission vital infrastructure cyber (MVI - C) and key terrain cyber (KT-C)
- How to ensure freedom of movement (FoM) and freedom of action (FoA) in cyberspace
- Identify the cyber risk to the mission
- Identify cyberspace opportunities
- Cyber resilience requirements
- Identifying the required cyber effects and predicting the unintended consequences
- Positive Identification
- How to operate in a cyber-degraded operational environment
- Which cyberspace actors are operating in the mission areas
- The capabilities and intent of the cyberspace threat actors

- How the adversary takes advantage of cyberspace to achieve their objectives
- The most likely course of action (MLCOA) and most deadly course of action (MDCOA) of the cyber threat actors.
- The need to collaborate with external stakeholders, including government, industry, and academia

COPD Process

Phase 1: Initial situational awareness of potential/actual crises

Phase 1 assists with the identification of potential or emerging crises. The initial understanding of the operational environment supports developing knowledge of all cyber aspects in the cyberspace area of interest and key terrain cyber. The commanders' critical information requirements (CCIRs) relative to cyberspace will be identified in this phase.

The cyberspace planner must consider things such as cyberspace actors, critical national infrastructure (CNI), government organisations and structures of friendly, neutral, and adversary actors. Products completed in Phase 1 include the PMESII/ASCOPE,[80] information requirements, and the cyber prioritised asset list (CPAL).

- **PMESII/ASCOPE:** The objective is to establish an understanding of the operational environment by identifying cyberspace knowns for analysis and unknowns for information requirements. This supports identifying factors such as mission vital infrastructure cyber (MVI-C), cyberspace actors, vulnerabilities, intent, capabilities, and locations.
- **Information requirements:** Information requirements related to cyber considerations are listed, such as essential elements of friendly information (EEFI), request for information (RFI), and CCIRs.
- **Cyber prioritised asset list (CPAL):** The CPAL is a list of prioritised critical assets essential to the mission. They are identified through the cyberspace terrain analysis process. It is a continuous process which identifies mission vital infrastructure cyber (MVI-C), critical national infrastructure (CNI), and mission relevant terrain cyber (MRT-C). An example of CPAL identification can be found in Annex B.

Phase 2: Operational appreciation of the strategic environment

Phase 2 begins with the receipt of the strategic warning order and the strategic assessment. This phase is carried out in two stages:

- **Strategic assessment:** This involves analysing the cyber considerations against the strategic situation and the desired end state, evaluating which

80 'PMESII/ASCOPE' stands for 'political, military, economic, social, information, infrastructure / areas, structures, capabilities, organisation, people, events'.

strategic cyber threats require attention or action at the operational level, and determining how these threats might impact the mission.

- **Military response options (MROs):** are considered from the perspective of cyberspace requirements and capabilities. MRO analysis can include:
    - An assessment of the joint operational area versus the cyberspace area of interest
    - What type of cyberspace operations are required, and what resources are needed?
    - Specific requirements for interaction with relevant national and international actors (government agencies, critical infrastructure, etc.)

In this phase, threat actor analysis is completed, which gives an overview of the cyberspace actors' capabilities. It may describe the actors and their goals, motivation, capabilities and what activates they have been previously involved in. It also describes what kind of threat the mission faces and which operational functions can be affected. The outcome of this is recommendations to mitigate the cyber risk to the mission.

Phase 3: Operational estimate – mission analysis

Phase 3 is divided into phases 3a and 3b. It assists the commander in determining what must be done to achieve mission success.

Phase 3a – Mission analysis

The mission analysis helps the cyber commander to establish a crisis analysis, determining which operational problem needs to be taken into account. In this phase, it is necessary to analyse how the conditions in cyberspace impact military activities and/or the achievement of the final operational objectives. Phase 3a will end with the mission analysis brief (MAB). Cyber considerations in this phase may include:

- What conditions must be established to achieve the operational objective
- What actions and effects are required to establish these conditions
- Synchronisation and inclusion of cyber actions and effects into lines of operations (LoO)
- Operational implications of time, space, and forces
- Which cyber capabilities are required
- What cooperation is required with other cyberspace actors in government agencies, MVI-C, CNI, etc.
- Identifying cyberspace operational risks and opportunities

The planners must know how cyberspace can create or support decisive conditions (DC), operational effects (OE), and operational actions (OA). The cyberspace centre

of gravity (CoG) analysis will also be conducted in this phase. **A centre of gravity (CoG) is defined as** 'the primary source of power that provides an actor its strength, freedom of action, or will to fight'

Phase 3b – Course of action (CoA) development
After the cyber commander planning guidelines, the cyber staff will develop the possible CoAs. This phase ends with the cyber commanders' decision on which CoA to develop, with a suitable final operational design, as the basis for developing a concept of operations (CONOPS).

At this stage, the risk assessment will be refined and cyberspace operational actions and effects will be identified for the different CoAs. Cyberspace operational actions and effects must be synchronised and deconflicted, as they may be connected to other domains.

Wargaming is conducted in this phase, which can result in identifying when or where cyberspace operations/actions can contribute to the mission.

Phase 4: Operational plan (OPLAN) development

This phase is split into two phases and details the cyber commanders' concept for the conduct of the mission and how the operational objectives will be achieved.

Phase 4a – Concept of operation (CONOP) development The cyber commanders' instructions for conducting a military operation in cyberspace are developed, together with the support of civilian and/or other entities, in order to achieve the operational objectives and establish the necessary conditions that contribute to achieving the strategic objectives and the respective desired end state. In this phase, command and control (C2) and the cyberspace scheme of manoeuvre (SoM) are also described.

The cyber commander also needs information about various stakeholders and/or partners involved in cyberspace operations (e.g. national cybersecurity centres, the private sector, and international partners).

Phase 4b – Operational plan (OPLAN) development is an interactive and collaborative process that focuses on synchronisation and coordination of the projection, employment, protection, support and sustainment of the operational force (e.g. cyber CISOPS/DCO/RRTs), during all phases of the operation and in a single plan at the operational level.

- A cyberspace operations order – or cyberspace annex, if it is part of joint operations – is developed. In these documents, a critical component is a

clear cyberspace concept of operations (CONOPS) and a cyberspace scheme of manoeuvre (SoM).

- An important aspect is that the cyber commanders' advice on legal and policy considerations, such as rules of engagement (RoE) and specific laws, could impact the planning and/or execution of cyberspace operations. Engagement with the LEGAD from an early stage is vital.

Phase 5: Execution

The objective is to manage the execution of the operational plan. It includes all operational level activities required to execute the operational plan, including assessing ongoing operations and, where necessary, reviewing the operational plan.

Assessment, measures of performance, and measures of effectiveness of cyberspace operations must be coordinated and integrated with the assessment of the overall mission. These will be discussed further in Section 5.4.

5.3 PLANNING CONSIDERATIONS

Authorisation Process

The authorisation and approval process for cyberspace operations differs depending on the type of operation.

For cyberspace operations that are not offensive in nature, authorisation and approval will generally but not always be at the operational level or lower and for cyberspace operations which are offensive in nature, authority and approval are typically at the political and strategic level.

Phases

In military operations, phases refer to the different stages of mission each with specific tasks and objectives that must be met before moving to the next phase. These phases provide structure, coordination, and strategic direction to achieve mission success, therefore, cyberspace operations must be planned and executed in synchronisation with other operational domains.

During each phase, cyberspace operations can be used to achieve decisive conditions. How cyberspace operations can contribute to and support the other domains must be considered against time, space, resources, and deployment. In addition, as cyberspace operations can be the main effort during any phase or point in time considerations such as preparation time, resources required and how the other operational domains can contribute and support cyber command to achieve its mission must be considered.

Timing

The cyber command must be aware that the timing of activities in cyberspace depend on the type of cyberspace operation being undertaken and the preparation that must be conducted. Different types of cyberspace operations have different timing considerations. CISOPS may have short preparation times if equipment is available and ready to be deployed. Similarly, DCO may be short if equipment, personnel, and memorandums of understanding are in place. OCO may require a long preparation time to gather intelligence, develop cyber tools/exploits, and get the required authorisation to execute. Once in position and authorised cyber effects can be achieved quickly.

In CISOPS and DCO, the speed of cyberattacks can occur quickly. Therefore, processes need to be developed which empower people at the appropriate level to take decisions quickly and implement effective countermeasures.

For OCO, DCO-EDM, and intrusive CyISR, preparation can require more time to evaluate the target and develop a CoA. In some cases, it can take weeks, months, or years from recognisance to weapon development and delivery. However, for a pre-prepared and authorised target, OCO can sometimes be conducted quickly.

Cyberspace operations must be considered as early in the planning process as possible. Cyber effects cannot be considered short notice options unless appropriate time considerations have been factored in as a result of prepared and pre-authorised actions.

Effects

In cyberspace operations, actions taken in the layers of cyberspace produce effects in the effect dimensions. A non-exhaustive list of cyber effects appears below.

- **CISOPS:** configure, extend, maintain, sustain, secure, block, isolate
- **DCO:** deter, deceive, contain, defeat, isolate, neutralise, recover
- **CyISR:** exfiltrate, manipulate
- **OCO:** manipulate, corrupt, exfiltrate, degrade, disrupt, deny, destroy

Due to the interconnected nature of cyberspace, the cyber commander needs to understand that cyberspace operations can produce first, second, and third order effects.

- **First order effects:** Direct consequences which have the immediate and intended outcomes of a cyber operation. Limited to the target itself or connected systems.

- **Second order effects:** Indirect consequences which occur as a result of the first order effect. For example, disrupting a power grid will have an effect on systems that rely on the power grid.
- **Third order effects:** Ripple or unintended consequences that were not originally considered or intended.

The ever-growing interconnected network of cyberspace creates an environment where unintended and uncontrolled effects can easily arise. This means that a seemingly low-level cyber operation, such as a temporary denial of service, might, due to unforeseen impacts, escalate to a level that could be considered a use of force or even an armed attack under the UN Charter and *jus ad bellum* (law on the use of force) principles.

Such escalation could give the adversary grounds to justify force in self-defence, whether individually or collectively. Assessing the impact of these effects involves criteria such as interference with critical infrastructure, the severity and reversibility of effects, and the level of invasiveness. The legality of a response ultimately depends on the specific context and actual effects of the cyberspace operation.

While unintended consequences are not unique to cyberspace, the extensive interconnectivity and interdependence between various networks – military, governmental, and private – increase the risk of such outcomes. This makes it essential, yet challenging, to assess potential collateral, cascading, and second or third order effects. Regardless of a commanders' risk tolerance, the commander must have a thorough understanding of these interdependencies and the possible impacts of the proposed cyberspace operation on normal network operations.

Information Sharing

In the cyberspace domain, establishing trust based relationships for effective information sharing is one of the primary challenges, particularly when it involves intelligence and offensive capabilities. Sharing sensitive information can mean sacrificing one nation's strategic advantage over others. Furthermore, national interests do not always align perfectly with those of alliances, creating potential friction in cooperative efforts.

However, information sharing is often more straightforward and mutually beneficial when it focuses on defending one's systems. In this context, nations and organisations can work together more easily to identify threats, improve defensive tactics, and strengthen collective security without compromising competitive advantages.

Two notable platforms facilitating defensive information sharing are the malware information sharing platform (MISP) and the cyber information and incident coordination system (CIICS). MISP allows users to document, share, and analyse malware and threat intelligence, which helps improve threat detection and prevention capabilities. Similarly, CIICS enables stakeholders to coordinate responses to incidents, share threat data, and register knowledge on cyber topics. Platforms such as these are essential in fostering collaboration, as they allow participants to use and build upon each other's knowledge, reducing duplication of effort and accelerating collective cybersecurity improvements.

Targeting and Positive Identification

Targeting is the process of selecting and prioritising targets and matching the appropriate response to them, considering operational requirements and capabilities.[81] Cyberspace targets can be considered according to the three effect dimensions and all seven layers.

Targets, along with the planned cyber actions and intended effects, must be validated early in the planning process according to the commanders' requirements. The main focus is on achieving the required objectives and effects.

Cyberspace targets are approved according to the joint targeting process. Coordination of these actions and effects should take place within operational and strategic targeting boards to ensure alignment with broader mission objectives. Additionally, all actions must be reviewed for compliance with relevant international and humanitarian laws. This requires personnel with specialised expertise who can identify potential targets, evaluate different courses of action, and assess risks and opportunities. By doing so, they enable the commander to select the most effective CoA, ensuring the greatest return on investment.

The targeting cycle in cyberspace should follow the same steps as those already established for all the other operational domains. It is a multidisciplinary effort and requires coordination, synchronisation, and deconfliction. This is achieved through targeting working groups, along with operational and strategic effects targeting boards. The output from the working groups can include the cyberspace contributions to the joint targeting list and the no-strike list, as well as how national and international law applies to the potential cyber actions against the target.

When considering targets in cyberspace, it is possible to know the virtual location of the target and not the physical location. As cyberspace operations can have cascading and compounding effects, it is possible that effects against a target can have effects outside the intended target, area of operations, or area of interest.

81 (US_AIR_FORCE, 2021).

Considerations during the targeting cycle include:

- **Rapid decision making:** Due to the speed of engagements, cyberspace operations require rapid iterations of the decision making cycle. One such decision making cycle is the observe, orientate, decide, and act (OODA) loop.
- **Deconfliction:** Coordination across domains makes it possible to avoid interference with other operations.
- **Adversaries:** Adversaries can adapt quickly, requiring real time updates which may require changes to the CoA.
- **Legal constraints:** Targeting must be conducted in a manner which ensures compliance with the applicable legal framework, in particular, international humanitarian law.
- **Ethical constraints:** It must also be conducted in order to ensure that any risk of civilian casualties or collateral damage is proportionate to the expected military advantage gained.
- **Avoiding physical damage:** For some targets, cyber capabilities may be the preferred option due to their lack of associated physical damage.
- **Security classification:** Coordinating cross domain fires requires careful attention to the security classifications of some cyber capabilities.

Cyber capabilities often allow targets to be engaged without causing permanent damage. However, the interconnected nature of cyberspace means that cyber effects may lead to unintended consequences if not thoroughly planned and coordinated.

Every target has unique inherent or acquired characteristics. These characteristics also help determine a target's value within a larger system and guide classification for future monitoring, analysis, engagement, and assessment.

Positive identification (PID)
A PID is a recognition derived from observation and analysis of target characteristics, including visual recognition, electronic support systems, non-cooperative target recognition techniques, identification friend or foe systems, other physics-based identification techniques, or human identity-based biometric data collection devices.

A PID provides the reasonable certainty that a functionally and geospatially defined entity is a valid military objective. An example of PID considerations can be found in Figure 5-1 aligned to the effect dimensions and the layers of cyberspace.

FIGURE 5-1 CYBERSPACE OPERATIONS GENERAL PID

Cyberspace Operations General PID Criteria and Example		
Effect Dimension	**Cyberspace Layer**	**Identification Examples**
Cognitive	Cognitive	Identifying users or administrators who interact with and provide the target function.
	Social	Recognising forums, online communities, and social interactions that contribute to or support the targeted function.
Virtual	Cyber Persona	Identifying virtual accounts, usernames, email addresses, or authentication credentials associated with the target function.
	Information	Protocols that are used to establish and maintain connectivity between logical elements. Recognising specific software, applications, configurations, or encryption services related to the targeted system.
Physical	Network Infrastructure	Identifying MAC addresses, IP addresses, VLANs, and VPN connections related to the target system.
	Physical Infrastructure	Identifying routers, switches, repeaters, servers, and endpoints physically supporting the target system.
	Geographic	Determining the precise geographic location of infrastructure supporting the target function.

5.4 ASSESSMENT

Establishing metrics for effectiveness is essential, as it enables the calculation of success rates for cyberspace operations and estimates of collateral damage, helping ensure that decisions are made with the best available information.

Several assessments should be conducted by the commander and their staff when planning and executing cyberspace operations. It is critical to measure whether the planned outcomes align with criteria set by the relevant review boards and through the estimation process. These assessments provide valuable feedback for refining future operations and help ensure progress toward the commanders' end state objectives.

Furthermore, there should be established metrics of effectiveness that enable the calculation of success rates for the different cyberspace operations and of collateral damage estimates so as to enable the decision to be taken in the most informed way.

There are a number of assessments that a commander and his or her staff should take into account when conducting cyberspace operations. A commander should seek to measure whether the planned outcomes have been achieved against criteria set by the various boards and the estimate process. Such measurements should seek to inform future iterations of the cycle and the commanders' end state objectives.

Targeting Assessment

For a targeting assessment to be effective, preparatory work must be done well in advance of the delivery of effects. This starts with the target system analysis (TSA), which identifies and prioritises targets to best exert influence on a system and thus to instruct which elements, criteria, or conditions should be monitored to inform the targeting assessment, and which intelligence sources are best suited to collect data based on those indicators. In targeting assessments, it is essential to gain an understanding among other considerations the following which will be expanded upon in future NATO CCDCOE publications such as the Handbook on cyberspace operations:

- Measures of performance (MoP)
- Measures of effectiveness (MoE)
- Effects assessment
- Combat assessment
    - Battle damage assessment (BDA)
    - Munitions effectiveness assessment (MEA)
    - Future targeting and re-attack recommendations
- Collateral damage estimate (CDE)
- Collateral effects estimate (CEE)
- Positive identification (PID)

6. Cyberspace Topics

6.1 CIVIL-MILITARY COOPERATION (CIMIC)

The nature of cyberspace has introduced challenges to traditional security frameworks. A significant amount of the infrastructure which governments and the military rely on is owned and operated by private entities, while much of the expertise and technological developments in cyberspace can be found in industry and academia. Additionally, government agencies are often the national agencies in cybersecurity legislation and governance.

Cyberspace threat actors often target critical infrastructure, blurring the distinction between military and civilian environments and creating overlapping responsibilities. As previously described, key terrain cyber (KT-C) and mission-vital infrastructure cyber (MVI – C), essential for mission assurance, often fall outside the direct control of the military. A cyberattack on this infrastructure can lead to mission failure.

Cyber threats can come from a variety of sources, such as state actors or those engaged in crime or espionage. Building trust and fostering cooperation between the military, government agencies, industry, partnerships, and academia is essential to addressing the challenge effectively. This aligns operational needs with the required resources, increases the availability of qualified personnel, and ensures freedom of movement in cyberspace. As cyberspace is a global domain, the demand for national and international cooperation becomes even more urgent. Global problems require global solutions, encompassing a whole of society and whole of system approach. However, global frameworks for cybersecurity remain underdeveloped.

Civil military interaction strengthens cyberspace operations by maintaining access to cyberspace, securing cyberspace assets, and enhancing resilience.

FIGURE 6-1: SPECTRUM OF CIVIL-MILITARY COOPERATION IN CYBERSPACE



Cyberspace civil-military cooperation embraces the following focus areas, national, international, industry, and academic cooperation.

National cooperation.

National civil-military cooperation involves coordination between public entities, such as government agencies, national security agencies, intelligence services, law enforcement, cyber command, critical infrastructure, and civilian cybersecurity companies. To ensure efficiency and avoid unnecessary duplication, the roles and responsibilities of military and civilian entities must be clearly delineated.

National collaboration between agencies enhances the ability to detect and respond to cyber threats by:

- Improving threat awareness: Defence, law enforcement, and national cybersecurity centres contribute unique perspectives that collectively enhance the understanding of potential cyber risks.
- Facilitating attribution: Sharing forensic evidence, threat intelligence, and indicators of compromise improves the ability to attribute cyberattacks, especially those involving state sponsored actors.

- **Key components in national cyberspace CIMIC include:**

    - Aligning national cybersecurity frameworks and strategies.
    - Policy and legal coordination.
    - Collaborating with government agencies and critical infrastructure.
    - Public-private partnerships: ensuring cybersecurity contracts, and cyber threat intelligence sharing.

- Incident response and crisis management: During cyber incidents or military operations, military cyber units often assist civilian agencies by providing technical assistance and supporting the restoration of critical infrastructure.
- Conducting joint training programmes and capacity building initiatives to enhance operational coordination and mutual understanding.

International cooperation.

In an increasingly interconnected world, cyber threats often transcend national borders, affecting multiple countries simultaneously. International cooperation is crucial for coordinating responses, sharing intelligence, and enhancing global cyber resilience.

Key components in international cyberspace CIMIC include

- Information sharing and intelligence collaboration: Facilitating the exchange of threat analysis, attribution data, and situational awareness to combat global cyber threats.
- Coordination: Facilitating coordination through multilateral organisations such as NATO, the European Union, regional bodies internationally, and the United Nations harmonises international efforts and builds collective cybersecurity capacity.
- Enhancing trust in cyberspace: Promoting transparency, confidence building measures, and shared norms helps reduce misperceptions and prevent escalation.

Industry cooperation.

Cyberspace is fundamentally a technological domain. Industry owns and operates much of the infrastructure. In addition, it holds a significant amount of the knowledge and capability in cyberspace. Therefore, there should be a dedicated research and development branch within cyber command to identify relevant technologies, products, and companies. This branch should maintain communication with cybersecurity and defence related companies, think tanks, and scientific forums. It should test cutting edge products and technologies based on the needs of cyber command and develop a catalogue of potentially suitable products and technologies.

Key areas of CIMIC cooperation with industry include

- **Provision of technology, equipment, and capabilities:** Partnering with private companies to acquire cutting edge technologies tailored to military needs.

- **Public-private partnerships:** Collaborating on joint initiatives for cybersecurity, including research, intelligence sharing, and incident response.
- **Critical infrastructure protection:** Working with private operators to secure essential systems, such as power grids and communication networks, against cyber threats.
- **Cyber threat intelligence sharing:** Ensuring real time exchange of threat data between industry and military entities.
- **Joint training and exercises:** Including private sector experts in cyber defence simulations to improve interoperability and readiness.
- **Innovation:** Supporting research and development in emerging technologies, such as artificial intelligence (AI) and quantum computing.
- **Building trust:** Strengthening relationships between military and private sector stakeholders to ensure effective collaboration.

Academic cooperation.

Academic institutions are vital to civil-military cooperation, providing research, education, and expertise in cybersecurity and emerging technologies. Universities often bridge the gap between theoretical knowledge and practical military needs.

Key areas of civil-military cooperation with academia in cyberspace include

- **Cybersecurity solutions:** Developing innovative tools and strategies to address evolving cyber threats.
- **Emerging technologies:** Conducting research into artificial intelligence (AI), blockchain, quantum computing, and other transformative technologies.
- **Case studies and scenario modelling:** Analysing past cyber incidents and modelling hypothetical scenarios to inform military strategies.
- **Education and workforce development:** Offering certifications, degree programmes, and professional military education (PME) to enhance the skills of military personnel.
- **Workshop and conferences:** Hosting events to promote knowledge exchange and collaboration between academia and the military.

6.2 QUANTUM TECHNOLOGY

The term ‘quantum technology’ is used to describe a new class of technologies that make use of the principles set forth by quantum mechanics, which is the fundamental theory in physics that describes the behaviour of particles at the smallest scale. This technology exploits unique quantum phenomena, such as superposition, entanglement, and quantum tunnelling, to create devices and systems with capabilities that go beyond

those of classical (or conventional) technologies. In short, quantum technology makes the unthinkable possible.

Quantum technology encompasses a number of distinct fields, including quantum computing, quantum communications. This technology is expected to have a profound impact on numerous fields, offering unprecedented computational power, enhanced security, and highly sensitive measurement capabilities. It can lead to breakthroughs in science, medicine, finance, and various industries, which can have a significant impact on society and the economy. It is a strategic technology that must be considered for future cyberspace operations because it will have a significant impact on cybersecurity.

Post-Quantum Cryptography (PQC): Preparation for Quantum Computers

It is particularly important to recognise that quantum computers, the most representative field of quantum technology, have the potential to have both positive and negative effects once they are developed. From a cybersecurity perspective, quantum computers have the capability to crack many of the passwords and authentication technologies used in all networks, including the internet. They can also be used as a powerful weapon to unsecure the secrets and personal information of an organisation without the need for espionage or hacking. This has been demonstrated by mathematical algorithms developed decades ago by mathematicians who anticipated the development of quantum computers. There is, however, still considerable debate over when quantum computers will emerge as a real threat. Nevertheless, there is no doubt that they will emerge. Therefore, it is imperative that we adopt a proactive approach to preparing to prepare for this significant threat.

The world is engaged in the research and development of novel mathematical techniques with the objective of eliminating the adverse effects of the advent of quantum computers and replacing current cryptography and authentication techniques, which we refer to as post-quantum cryptography (PQC). The United States National Institute of Standards and Technology (NIST) is spearheading the initiative to standardise PQC algorithms. The United States government, including agencies such as the National Security Agency (NSA) and the Cybersecurity Agency (CISA), is encouraging government organisations to prepare for the transition to post-quantum cryptography by establishing a quantum readiness roadmap and collaborating with technology vendors. In recent times, the European Commission has published a coordinated implementation roadmap for the transition to PQC. This publication recommends the development and implementation of national PQC transitions, with the objective of ensuring interoperability across EU countries. A significant number of countries have already published national roadmaps, initiatives, and other measures

aimed at developing PQC technologies and ensuring systematic preparedness. In line with this trend, it is of paramount importance for the military to prepare a systematic readiness plan to enable the early application of post quantum cryptography (PQC) technology in order to protect vital military or secret information in collaboration with the government and the military of allied countries.

Quantum Key Distribution (QKD): Utilisation of Quantum Communication

Quantum communication technology represents a promising avenue for the advancement of secure digital communications and infrastructure. A range of technologies exist, yet for the sake of efficiency, safety, and reliability, it is prudent to consider the utilisation of quantum key distribution (QKD). QKD is a technology that employs the principles of quantum mechanics to facilitate the secure sharing of cryptographic keys between two entities. The detection of eavesdropping during the key distribution process makes QKD a more secure technology than traditional key distribution methods (such as PKD, or public key distribution). Furthermore, it is a secure technology for the advent of quantum computers. There are numerous research projects on secure key distribution protocols and infrastructure construction projects for communication and practical use employing optical fibre networks in Europe, China, and the United States. Research on QKD in space using repeaters, wireless QKD, or QKD satellites to overcome distance limitations is also being promoted. Additionally, the most crucial issue in military secret communication is the pre-key sharing for encryption, and the utilisation of QKD technology will contribute to enhancing the security level of future military operations. The QKD-related security and network equipment industry is also experiencing continuous expansion. It is therefore incumbent upon cyber commanders' to monitor and assess the ongoing increase in functionality and cost effectiveness.

It is not within the mission of cyber commanders' to engage in direct research or development of quantum technologies. Rather, it is incumbent upon them to foster collaboration and information sharing with national counterparts and international allies with a view to developing and implementing joint defence strategies aimed at safeguarding military infrastructure and data that may be vulnerable to quantum technologies. Furthermore, conducting cyber simulation exercises and training based on cyber threat scenarios exploiting quantum computers can serve as a proactive measure to enhance response capabilities for real world situations. It is evident that these endeavours cannot be achieved without the cyber commanders' comprehension of and interest in quantum technology.

6.3 THE CYBER-HYBRID INTERSECTION

Cyberspace plays a special and very specific role as an operational domain. Everything significant that happens in the real world, including every political and military conflict, will also take place in cyberspace (and has already). For national security planners, this includes cybercrime, propaganda, espionage, influencing, terrorism, and even warfare itself. The nature of national security threats has not changed, but cyberspace has provided a new delivery mechanism that can increase the speed, diffusion, and power of an attack – and is even anonymous. Its ubiquitous and unpredictable characteristics mean that the battles fought in cyberspace can be just as important – if not more so – than events taking place on the ground.

Since 2016, NATO and the European Union (EU) have identified countering hybrid threats as a priority for cooperation. The most tangible effects were the establishment of a Hybrid Fusion Cell as part of the EU Intelligence and Situation Centre, a Hybrid Analysis Branch as part of NATO, and a European Centre of Excellence for Countering Hybrid Threats.

The combination of cyber power and hybrid threats represents an explosive blend of factors that has enabled adversaries to leverage their relatively meagre resources. For western strategists and decision makers, this means that the traditionally weaker part of the adversarial equation has now received additional advantages and opportunities through the hybridisation of modern warfare. For several years, the term 'hybrid threats' has increasingly been used to explain the nature of threats, including the nature of war. However, this excessive use and monograph also call into question whether it is a meaningful characterisation of the threats we face.

It seems more important to clarify the ambiguities at the strategic level, as these will only blur further in the event of threats from cyberspace or hybrid threats. Such vagueness is most clearly expressed when the scientific debate speaks of hybrid threats and refers to cyberattacks, which are only part of a broad spectrum of hybrid means. Nevertheless, there are relatively specific characteristics that differentiate hybrid from cyber threats.

Cyber threats refer to those activities in cyberspace that have hostile intent or have criminal or destructive consequences. The nature of cyber threats derives from the unique characteristics of cyberspace. Among the operational domains, cyberspace plays a unique role. Unlike the other domains, cyberspace is the product of deliberate human action. It consists of various hardware and software components that have been woven together in a global network. As such, cyberspace can change rapidly, whereas conditions in the maritime environment, in the land, air, and in space are

relatively constant. Nowadays, cyberspace's seamless functioning has become the most critical prerequisite for operations in all global commons. Cyberspace is a key enabler for actions in other operational domains.

However, cyberspace is hybrid in nature. It is neither owned nor operated exclusively by public or private actors. Because cyberspace is the glue that binds together individuals, states, and companies, everyone has a stake in securing it. Therefore, advancing cybersecurity requires close public private and civil military interaction on a whole of society approach because inadequate cybersecurity governance risks cutting modern societies off from the benefits of access to the global commons.

Cyberspace represents a domain and critical infrastructure. Furthermore, it is a tool or even a weapon to cause damage. Cyberspace operations allow an adversary to seek a broad spectrum of actions. They range from small scale espionage operations to system observation, to larger scale destruction of physical elements up to taking control over the C4 system (command, control, communication, and computers) of the attacked armed forces / society / state.

Hybrid threats refer to the methods and tools used by individual state or non state actors to enhance their interests, strategies, and goals. The range of methods and activities is wide: it includes influencing information and propaganda, logistical weaknesses like energy supply pipelines, economic and trade related blackmailing, undermining international institutions by rendering rules ineffective, and terrorism.

Hybrid threats are methods and activities that are targeted towards the vulnerabilities of the opponent. Vulnerabilities can be created by many things, including historical memory, legislation, old practices, geostrategic factors, the strong polarisation of society, technological disadvantages, or ideological differences. If the interests and goals of the user of hybrid methods and activity are not achieved, the situation can escalate into hybrid warfare, where military and violence will increase significantly.

Hybrid threats are a very common combination of activities leading to consolidated impacts involving two or more domains and leveraging the conventional and non conventional means of attacks and/or instruments.

Accordingly, the Hybrid CoE characterises hybrid threat as:

- Coordinated and synchronised action that deliberately targets democratic states' and institutions' systemic vulnerabilities through a wide range of means.

- Activities that exploit the thresholds of detection and attribution, as well as the different interfaces (war/peace, internal/external security, local/state, and national/international).
- Activities aimed at influencing different forms of decision making at the local (regional), state, or institutional level and designed to further and/or fulfil the agent's strategic goals while undermining and/or hurting the target.

Thus, hybrid threats are harmful activities that are planned and carried out with malign intent. They aim to undermine a target, such as a state or an institution, through a variety of means, often combined. Such means include information manipulation, cyberattacks, economic influence or coercion, covert political manoeuvring, coercive diplomacy, or threats of military force. Hybrid threats describe a wide array of harmful activities with different goals, ranging from influence operations and interference all the way to hybrid warfare.

Hybrid threats aim to restrict the political room for manoeuvre by targeted states, including by undermining their citizens' sense of security. They are designed to create fear or anxiety and sow distrust towards authorities and other people, citizens, or groups. They target and exploit vulnerabilities inherent in democratic systems of government and in the fabric of democratic societies, such as political rights and individual liberties. By using hybrid threat activities, malign actors seek to drive wedges into society and to undermine social cohesion and trust among citizens and towards their democratic institutions.

6.4 THREAT DISCOVERY (THREAT HUNT/EMULATION AND PURPLE TEAMING)

Threat discovery is the combined use of threat hunting and threat emulation to proactively identify and defeat adversary activity within organisational systems. This section is a generic explanation of threat discovery and not a guide on establishing a threat discovery capability. This section demonstrates a potential vehicle that operates under a constant assumption of successful adversary infiltration and identifying skill perishability and potential talent and educational issues.

Threat Hunting

A viable threat hunting capability can provide early detection of suspicious activities, which can be instrumental in disrupting adversary cyberspace operations.[82] Working on the assumption that adversaries have already infiltrated the network, threat hunting is the proactive discovery of undetected adversaries within a network. It is not as simple as looking for tactics, techniques, and procedures and indicators of compromise. Threat hunters should not configure network defences nor conduct offensive actions,[83]

82 (Cyber Diia Platform, 2024)
83 (Maxam & Davis, 2024)

in fact mature threat hunting capabilities work on behaviours rather than TTPs and IoCs[84] Commanders' with a correctly developed threat hunting capability can enhance incident response by strengthening cybersecurity posture and resilience.[85]

Threat hunting expertise is subjective, as it requires skills from across multiple cybersecurity disciplines. While industry courses exist that can build skills, there are currently no standardised education pathways for training threat hunters, particularly in a military context. Anecdotally, proven threat hunters generally have strong cybersecurity specialty knowledge and a mixture of behavioural traits like patience, diligence, and perseverance. Procedurally, successful threat hunting requires a structured repeatable process which begins by gathering intelligence and information to build a hypothesis and determine data sources.[86] This process can be significantly streamlined when supported by timely cyber threat intelligence that provides specific behaviour identification and information on system vulnerabilities. A successful capability can be built, provided the capability is based on strong methodologies and skilled knowledgeable personnel.

Effective threat hunting requires contemporary understanding of deploying information and communication technology infrastructure pre-deployment, including backbone systems that facilitate interaction with broader (inter)national systems. The best practice is to baseline conventional system activity to better identify the abnormal, such as mapping systems against the Mitre ATT&CK framework.[87] Even where large amounts of security data are captured, understanding if the available data answers the required queries requires expertise.[88] This expertise is crucial for threat hunters to understand what data sources are available to validate and identify anomalous activity, such as which logging is turned on and captured, Sysmon availability, and so on. At a minimum, threat hunters should be given adequate time to keep themselves up to date on system knowledge and methodology, and where practical, given the time to fully appreciate the systems they work on.

Finally, just having the correct processes and personnel in place is inadequate without the correct authorities to act. Prior to any deployment or response activity, predetermined authority – i.e. pre-approved actions – must be considered and, where possible, be put in place. Threat hunters should have the relevant permissions and accounts to operate across interacting systems direct from the relevant authority or memorandums of understanding in place with relevant system owners. This allows threat hunters to commence work proactively or at the earliest identification of potential threats.

84 (CISA C. &., Nation-State Cyber Actors, 2025)
85 (Fortninet, 2023)
86 (Bianco, 2023)
87 (Mitre ATT&CK, 2024)
88 (Legg, 2024)

Threat Emulation

Emulating the adversary provides defenders with a view of the network from an attacker's perspective.[89] It must be noted that threat emulation differs significantly from penetration testing. While both take offensive actions that simulate an adversary, penetration testing identifies vulnerabilities around the edge of the network, while threat emulation actually infiltrates into the network.[90] The importance of this distinction lies in the fact that actual infiltration of the network provides valuable data to defenders.

A threat emulation capability is intended to realistically simulate adversary attacks on the network to identify weaknesses and improve prevention and detection response.[91] Due to the dynamic nature of the threat, i.e. critically rated common vulnerabilities and exposures (CVE) occurring almost daily, a threat emulation capability must be agile.[92] Therefore, in order to provide a thorough examination of cyber defences, threat emulation resources must have a comprehensive understanding of adversary tactics, techniques, and procedures (TTPs) across the attack lifecycle, i.e. reconnaissance to exfiltration. This thorough comprehension is best achieved via a strong cyber threat intelligence (CTI) input to threat based adversary emulation. This combination enables threat emulation to achieve significant results that can be further enhanced when used in conjunction with the defensive capabilities, i.e. purple teaming.

Purple Teaming

Described as cyber threat intelligence led offensive operations to improve security posture, foster collaboration, provide learning opportunities, and bolster defensive detection,[93] purple teaming is a comprehensive and collaborative approach to cybersecurity that provides adaptable methodologies for evolving cyber threats.[94] By combining red and blue team methodologies and processes, i.e. offensive and defensive, an organisation creates a strong cybersecurity operations capability.[95] This capability enhances an organisational ability to quickly identify and address security risks by providing insight not achievable by a single team.[96] Done correctly, purple teaming can drastically enhance an organisations capability to proactively improve prevention, detection, and response mechanisms. Effective purple teaming should be the goal of cyber commanders', as it is also the sign of a mature threat discovery capability and therefore strong protection against adversary offensive operations.

89 (Ajmal A.B, 2021)
90 (Maxam & Davis, 2024)
91 (SANS, 2024)
92 (Magnusson, 2023)
93 (Olsen, 2022)
94 (VanBuggenhout, 2024)
95 (Ilca Lucian & Balan Titus, 2022)
96 (Steshenko A. , 2023)

6.5 CYBERSPACE RESILIENCE

Cyberspace is continuously contested, and we must assume that eventually, a cyber incident will occur, causing systems we rely upon for daily operations to have reduced functionality or be unavailable. Military systems must perform their mission in the face of threats and under extreme conditions.[97] Resilience is key to ensuring that these systems and processes can recover and continue to operate when cyber systems have been affected by either unintentional or malicious activity.

While traditional risk management methods have been effective for simpler systems, recent years have seen a growing recognition of their limitations. This has led to a shift towards a resilience based approach, which offers a more comprehensive understanding of risk. The traditional method, which quantifies risk as the product of threats, vulnerabilities, and the impact of an undesirable event, is increasingly seen as inadequate for complex and interconnected cyber systems.

Risk = Likelihood x Impact

Even if we know the impact of an event, that does not tell us how well the system is able to absorb an event such as a cyberattack or how quickly and how well the system can recover. Cyber capabilities are typically based on increasingly complex and interconnected systems. Due to the interdependency, the consequences can easily spill over to other systems, causing unexpected cascading effects. Quantifying risk in the traditional manner for such a complex system can be impossible, and the possible results have so much uncertainty that they are of limited use in practice. The resilience based methods introduced in this section represent different approaches towards using resilience and how they can be used in a quantitative way and with a focus on the mission. The text of this section draws extensively from the book Cyber Resilience of Systems and Networks (Kott and Linkov, 2019), as many of the book's authors are leading experts in their respective fields and together provide an overview of the various aspects of resilience.

Resilience versus traditional risk management

Risk-based strategies are most effective when hazards are known and their probabilities can be estimated. These strategies become problematic when hazards are unknown, interlinked, or difficult to estimate or when they can cause extensive damage, often indirectly, through cascading effects.

Resilience focuses on the ability of a system to continue to fulfil its purpose in the face of incidents degrading its performance and then recovering, irrespective of the cause. But using resilience successfully requires a good understanding of the mission

97 (Crossett, 2019)

and how it depends upon the system in question, e.g. the system's boundaries and performance and the appropriate timeframe.

Robustness is another concept (besides risk) often confused with resilience. Robustness is closely related to risk. Robustness denotes the degree to which a system is able to withstand an unexpected internal or external threat or change without a degradation in system performance.

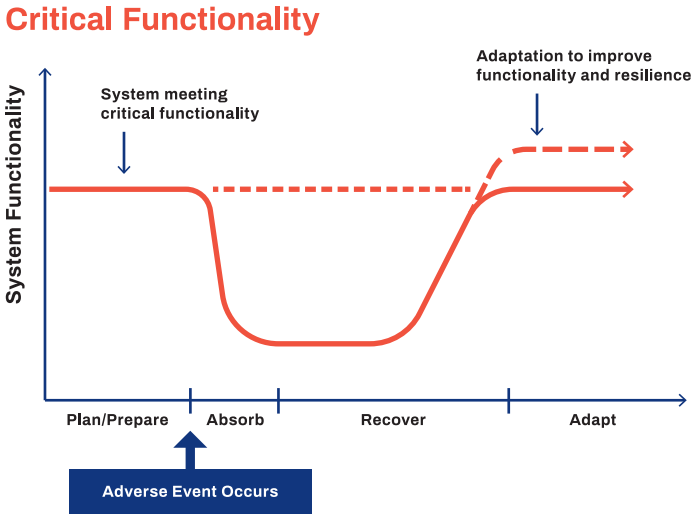
Traditional risk management starts by assessing the likelihood of an undesirable event, evaluating its potential consequences, and identifying possible mitigations. This process is then repeated as necessary. The underlying assumption (whether people realise it or not) will often be to prevent the event from occurring. All the effort goes into making the system robust; what is neglected is resilience, the system's ability to recover.

Thus, there has been increased interest in approaching risk management on a resilience basis, beginning by focusing first on the impact and the recovery process and then focusing on the likelihood of an undesirable event. The advantage of this approach is that it is a more robust way of dealing with consequences, but it can also deal better with uncertainties in likelihood for complex systems because it becomes easier to get results that depend less on accurate likelihood estimates. When resources are limited, it is a definite advantage to be able to put the most effort into factors that can be estimated and reduce the importance of factors that are difficult (sometimes impossible) to estimate accurately.

The concept of resilience is used in many different fields. Slightly different definitions are employed in each, but a common definition is the ability of a system to **plan/ prepare, absorb, recover, and adapt** to changing conditions. There are features of resilience common to many fields such as socio-ecology, psychology, organisations, and engineering and infrastructure. These are related to the temporal phases from the US National Academy of Sciences' definition of resilience: plan, absorb, recover, and adapt.[98] The following figure 6-2 describes the phases of dealing with an adverse event using a resilience based approach:

98 (Kott & Linkov, 2019)

FIGURE 6-2: NOTIONAL RESILIENCE PROFILE, PLOTTING A SYSTEM'S CRITICAL FUNCTIONALITY OVER TIME (KOTT & LINKOV, 2019)



Risks cannot be eliminated. Therefore, military systems must endure long-term threats from various sources, such as environmental factors and sophisticated cyberspace adversaries. The concepts of recovery time objective (RTO) and business continuity (BC) must be built into all CISOPS activities, just as cyber and information security are. Business continuity is essential for organisational resilience. From the perspective of cyberspace resilience, Business continuity may mean having alternative systems or manual processes in place to absorb the loss of functionality while the primary systems are restored to normal operation.

To maximise resilience against attacks for military systems, two strategies are essential:

- **Increase the cost for the adversary:** This involves making attacks more resource intensive and difficult to execute, including the effort required to develop, access, traverse, and maintain an attack.
- **Decrease the impact of attacks:** This means ensuring that systems can still perform during an attack, either by reducing capacity, transferring missions to other components/systems, or finding alternative methods.

Chuck Crossett[99] argues for a 10 step guidance for the cyber resilience of military systems:

99 (Crossett, 2019).

- Design resilience to cater for a cyberspace adversary in a similar manner to how you design physical defence for kinetic adversaries.
- Design out vulnerabilities as much as possible.
- Increase the cost for the adversary to get into your system.
- Increase the cost for the adversary to get around inside your system.
- Know what is going on in the system at all times.
- Decrease the impact of the attack.
- Include recovery and reconstitution of the system in your resilience scheme.
- Assess and test constantly.
- Protect the system as you build it.
- Protect the system as you operate and maintain it.

This could be expanded to include some additional ideas from Bodeau and Graubart's (2011) framework of cyber resiliency, such as manage complexity, choose topology, add resources, and design for reversibility.

Conclusion: The objective of resilience is to enable IT systems to absorb the impact of cyber incidents and recover quickly. This involves designing systems that can withstand attacks, maintain business functionality during an attack, and rapidly restore full operational capabilities afterwards.

Cyber commanders' are essential in instilling a culture of resilience across all levels of military planning and operations through strategic planning, operational readiness, system design and acquisition, and continuous improvement. By fostering this culture, cyber commanders' can ensure that military operations continue seamlessly despite cyberattacks. This approach is crucial for maintaining operational integrity and effectiveness, as cyber incidents are inevitable. Embedding resilience at every level of military operations helps maintain mission readiness.

6.6 HOW AI IS CHANGING CYBERSPACE OPERATIONS

As artificial intelligence (AI) advances, its integration into cyberspace is fundamentally reshaping how cyberspace operations are conducted, both defensively and offensively. With AI's ability to process and analyse data at unprecedented speeds, it is revolutionising the way we detect, respond to, and even carry out cyberattacks. As both cyber defenders and attackers leverage this powerful technology, it becomes clear that AI will be central to future conflicts. This section explores how AI is transforming defensive cybersecurity operations and offensive tactics, techniques, and procedures (TTPs) and how large language models (LLMs) are changing the modern battlefield.

Artificial Intelligence for Defensive Cyberspace Operations

In cybersecurity, defenders face increasingly sophisticated and frequent threats that challenge traditional systems. AI provides an answer to these challenges by automating threat detection, response, and even prediction, drastically reducing the time needed to react to breaches and attacks. The combination of AI and machine learning (ML) enables security systems to learn from past incidents and adapt to new threats with far greater speed than human operators. AI's ability to analyse vast datasets allows it to identify malicious patterns often missed by human analysts. For instance, AI-powered behavioural analytics models monitor user activity and network traffic, identifying anomalies that could signal a cyberattack. Real-time intrusion detection systems (IDS) leverage AI to constantly monitor networks, isolating suspicious activities before they escalate and even predicting future attack patterns by learning from previous threats. Beyond detection, AI automates responses to cyberattacks. When threats are identified, AI-driven systems can immediately isolate affected network parts, terminate malicious processes, or roll back to secure states, minimising potential damage. This has transformed incident response from a manual, reactive process to a proactive one that involves continuously learning and adapting to new threat vectors. While AI significantly enhances cybersecurity defences, its implementation faces several challenges. Interoperability between heterogeneous systems in cyber defence networks is a major technical hurdle, as ensuring seamless communication between multiple AI components is complex. Moreover, AI systems themselves are vulnerable to adversarial attacks, where malicious actors manipulate input data to cause incorrect predictions or missed threats. This necessitates the continuous adaptation of cybersecurity frameworks. AI-driven incident response systems, though highly effective in detecting and mitigating threats like ransomware, require large, diverse datasets for training, which can be difficult to obtain due to varying data formats. The risk of false positives or negatives persists: legitimate activities might be flagged as malicious or real threats overlooked. Ethical concerns further complicate AI's use in cybersecurity, as AI-based surveillance systems may infringe on privacy rights, and autonomous defence systems could lead to unintended consequences if they misinterpret situations. Balancing AI's powerful capabilities with these technical, operational, and ethical challenges remains crucial in the evolving landscape of cybersecurity.

Artificial Intelligence for Offensive Cyberspace Opeations

While AI is an invaluable tool for defenders, it is equally powerful for attackers. Offensive cyberspace operations, which include hacking, malware deployment, and network penetration, are becoming more sophisticated with the integration of AI. The same attributes that make AI useful for defence – automation, speed, and adaptability – are now being harnessed to create more effective and dangerous cyberattacks. AI can dramatically enhance offensive cyberspace operations by automating tasks

that traditionally require significant human expertise and time. One of the most common applications is vulnerability scanning and exploitation. AI algorithms can scan networks and systems for weak points, identifying potential exploits far faster than human hackers can. Once a vulnerability is found, AI can automatically develop strategies to exploit it, streamlining the process of gaining unauthorised access. Phishing and social engineering attacks have also been transformed by AI. Traditionally, these attacks depended on deceiving victims into unknowingly handing over sensitive information. With AI, attackers can now craft highly personalised phishing emails that mimic the writing styles of trusted contacts. Furthermore, AI can generate real time human like dialogue, making it increasingly difficult for victims to distinguish between legitimate communications and sophisticated attacks. The scalability of AI allows attackers to conduct thousands of these personalised attacks simultaneously, significantly amplifying their impact. A notable development in offensive cyberspace operations is the emergence of AI-powered malware. Unlike traditional malware, which follows predefined instructions, AI-driven malware can dynamically adapt to its environment, evading detection and modifying its behaviour to out manoeuvre common cybersecurity defences. A prime example of this is IBM's Deeplocker, a form of malware that uses AI to conceal its malicious intent until it identifies a specific target. It employs methods such as facial or voice recognition to trigger its payload, making it far more elusive than conventional malware. Closely linked to this is the growing threat of adversarial AI, where attackers manipulate machine learning models to sabotage defensive systems. In these attacks, adversaries intentionally 'poison' data sets or machine learning algorithms used by cybersecurity defences, causing them to make erroneous decisions. This enables attackers to bypass security measures or, in some cases, manipulate the AI systems to act against their own organisations. Adversarial AI techniques can also introduce subtle perturbations into data that confuse classification algorithms, rendering detection mechanisms ineffective. This represents a significant escalation in the complexity of cyber warfare, as AI systems are increasingly weaponised to undermine one another. Reinforcing this trend is the application of reinforcement learning (RL), a subset of AI, to refine offensive cyber strategies. In this process, AI systems simulate different attack techniques in controlled environments, learning from both their successes and their failures. Over time, the AI hones its tactics, becoming increasingly adept at carrying out effective cyberattacks. These refined strategies can then be applied in real-world scenarios, further enhancing the sophistication of AI-driven offensive operations. In combination, these developments illustrate the escalating complexity and potential dangers of AI in the cyberspace domain, as attackers continually refine their methods, leveraging AI's adaptability and learning capabilities to outpace traditional defences.

How LLMs Are Changing the Modern Battlefield

Large language models (LLMs) such as GPT-4 have significantly advanced in their capability to understand and generate human like text, with profound implications for military strategy and cybersecurity. In military operations, LLMs are revolutionising decision-making processes by enhancing the analysis and processing of extensive datasets. They can sift through vast amounts of information, including intercepted communications and surveillance data, to identify critical patterns and security risks. By analysing historical conflicts, current battlefield conditions, and adversarial capabilities, LLMs support military planners in crafting more informed and strategic decisions, effectively accelerating the development of battlefield strategies that would traditionally require far more time and effort. In cybersecurity, LLMs are equally transformative. They play a pivotal role in both defensive and offensive operations. On the defensive side, LLMs automate the classification of threats, assist in generating detailed incident reports, and identify emerging trends in cyberattacks by processing language-based information and detecting anomalies in communications or code. This proactive capability often allows for the early detection of potential threats before they fully materialise. Conversely, on the offensive side, LLMs contribute to the development of cyberattack strategies by analysing historical data on successful attacks. They can suggest effective tactics, techniques, and procedures (TTPs) for exploiting current vulnerabilities, thus enhancing the precision and efficacy of offensive cyberspace operations. Integrating LLMs into high stakes domains like military strategy and cyberspace operations emphasises the need for effective human-AI collaboration. AI systems must be designed to complement human expertise with intuitive interfaces and transparent decision making processes. While AI accelerates data-driven insights, strong human oversight is essential to ensure that its recommendations are ethical, reliable, and aligned with broader goals. Achieving the right balance between AI and human judgement is key to leveraging AI's potential while mitigating risks in these critical fields. Moreover, the use of LLMs also introduces significant ethical and legal challenges. One major concern is the potential for LLMs to generate persuasive misinformation or propaganda, which could exacerbate conflicts and destabilise societies. Furthermore, the deployment of AI in autonomous weapons systems raises profound questions about accountability and human oversight in life and death decisions on the battlefield. Addressing these ethical and legal issues is essential to ensure that AI technologies are used responsibly and in ways that uphold international standards and human rights.

6.7 EXPERIENCE AND LESSONS FROM UKRAINE

As of the time of writing, Ukraine has yet to establish a centralised cyber command. The functions of cyber defence in Ukraine are currently spread across several agencies, including the General Staff of the Armed Forces of Ukraine, the Security

Service of Ukraine, the Main directorate of Intelligence of the Ministry of Defence of Ukraine, the Foreign Intelligence Service of Ukraine, and the State Service for Special Communications and Information Protection. Since May 2021, efforts have been underway to create a centralised cyberspace force within the ministry of defence[100] to improve coordination and efficiency in addressing cyber threats. Additionally, the ministry of defence has initiated efforts to define the term "cyber war" at the legislative level.[101] This raises important questions about the significance of cyberspace operations, particularly their potential to achieve both tactical and strategic effects.

Since 2022, the frequency of cyberattacks on Ukraine has risen significantly, originating from both state and non-state actors. In response, Ukraine's security and defence sector regularly publishes reports on cyber incidents.[102] These cyberspace operations aim to achieve both tactical and strategic objectives. They target Ukraine as well as partner countries, expanding opportunities to influence events on the battlefield while offering a significant advantage in the global political arena. The strategic goals include influencing political decisions, demoralising the population, and weakening international partnerships. Tactically, the attacks aim to disrupt critical infrastructure, obstruct state services, and create chaos.

The hybrid nature of the conflict enables the integration of multiple operational domains, maximising the effectiveness of available resources. The disregard for international law and humanitarian principles has led to frequent targeting of civilian infrastructure, causing cascading effects, long term infrastructure failures, and substantial economic losses. To mitigate these threats, Ukraine must allocate significant resources to detect, identify, neutralise, and recover from cyber incidents.

As the number of cyberattacks increases, it may seem at first that these attacks are disorganised. However, they serve as testing mechanisms for assessing Ukraine's response and recovery capabilities. Success or failure in these attacks can help identify higher-priority targets. The statistics from cyberspace operations on both sides suggest the presence of an initiative in this confrontation one that relies on having greater resources and using them effectively. Parties in the conflict focus on increasing their own capabilities and reducing those of the other side. Enhancing capabilities involves improving personnel, developing new tools and methods, and strengthening partnerships, while reducing an opponent's capabilities involves creating uncertainty and increasing risks.

Cyberspace operations also support informational and psychological warfare, enhancing the effectiveness of kinetic attacks. Conversely, kinetic operations can

100 (Parliament of Ukraine, 2021)
101 (Ministry of Defense Ukraine, 2024)
102 (cip.gov.ua, 2024)

facilitate cyberattacks. For instance, physical damage to infrastructure often prioritises recovery of functionality over cybersecurity, which may increase supply chain risks as information assets are moved. The private sector, which provides essential technical solutions, also plays a crucial role in cyberspace operations.

The scope of cyberspace operations extends beyond technical factors. One of the key aspects is control over the operations themselves, as losing control can result in negative consequences. For example, the NotPetya malware, which originally targeted Ukraine, had widespread effects beyond its intended target. The speed, consequences, and control over cyberspace operations referred to as the "Subversive Trilemma" are influenced by factors such as vulnerabilities, the human factor, and insider threats. Finding optimal solutions within this paradigm is a form of operational art.

An additional layer of complexity in the war is the presence of hacktivist groups, which introduce more uncertainty. These groups can impact cyberspace operations both positively and negatively, acting independently[103] or in coordination with state agencies.[104] Hacktivists can obscure state sponsored actions by taking responsibility for cyberattacks. They may also carry out operations under a "false flag" to create external conflicts, which is especially relevant given that cyber diplomacy is still in its infancy in many countries. Hacktivist groups often target civilian infrastructure for financial gain or to acquire sensitive data, such as customer databases. During wartime, data from services like taxis, food delivery, and medical labs can be particularly valuable. Correlating this data can identify military personnel, their families, and key strategic assets, posing real threats.

Time is a critical factor in cyberspace operations. The execution of an operation can be expedited by having sufficient information about the target and by preventing leaks during the planning phase. Leaks reveal the target, allowing preparations that can reduce the chances of success. Conversely, influencing the planning of cyberspace operations particularly in terms of agreeing upon and validating objectives can also be important.

The identification, agreement, and validation of cyberspace operation objectives are crucial, as they can influence other operational domains. However, these processes come with significant risks, such as conflicting interests among participants, compromised individuals, information gaps, insider threats, data leaks, and the loss of access to critical infrastructure. For example, if participants are compromised, cyberspace operations may face delays, and the need to replace personnel can lead to a loss of initiative, giving the opposing side an advantage. One way to mitigate this risk is by decentralising the functions of cyberspace forces among various entities,

103 (Davydiuk A)
104 (Butchenko, 2024)

though this approach carries its own risks, including competition, duplication, and poor coordination. Ukraine is working to minimise these risks.

In addition to threat intelligence, the intelligence activities of relevant state bodies are crucial to the success of cyberspace operations. Timely information about an adversary's presence within state systems or critical infrastructure can prevent or mislead harmful actions while also providing valuable insights into their tactics. This intelligence can enable the creation of countermeasures and mirror effects that neutralise the adversary's goals. Additionally, intelligence activities can help prepare for the integration of emerging technologies, such as artificial intelligence and quantum computing, into cyberspace operations.

Another important aspect of cyberspace operations is the dissemination of information about their effects. The scale of a cyberattack is not always immediately clear to the attacker, but understanding its impact is vital for planning subsequent actions. The repetition or escalation of effects after recovery can indicate the success or failure of the operation. Acknowledging participation in cyberspace operations, on one hand, risks focusing opposing efforts on de-anonymising participants and finding ways to neutralise them. On the other hand, it can serve as a demonstration of capabilities, contributing to deterrence. The spread of information about cyberattacks may also be part of a broader strategy to undermine public confidence in the government, creating a perception of insecurity and weak state institutions.

To effectively counter cyberspace operations and multi-domain operations, Ukraine is actively developing a regulatory framework for cybersecurity and critical infrastructure protection. This includes enhancing personnel training, conducting cyber exercises through cyber ranges, facilitating tabletop exercises, and advancing cyber diplomacy.

Conclusion

Cyberspace operations are an increasingly critical component in modern conflict. Cyberspace is a relatively new operational domain, one that continues to evolve, requiring constant adaption. While the concepts and ideas required to operate in this domain are becoming established, they are still subject to change. It is essential to harmonise cyberspace definitions and lexicon with internationally accepted terms and standards to ensure a common, unified understanding of cyberspace.

The cyber commander must be aware that doctrine and standard operating procedures will require regular review to ensure they align with international best practices. The ability to understand this environment, integrate cyber capabilities into operational planning, and effectively conduct cyberspace operations will be a force multiplier and play a decisive role in future conflicts. It will be important to integrate cyberspace considerations into the earliest possible stages of planning. In addition, authorities and approval processes should be exercised regularly so that the decision making processes can be refined and thereby increasing operational efficiency.

To achieve operational superiority, cyber commands must continuously adapt, leveraging new and emerging technology such as artificial intelligence (AI) and quantum computing when conducting operations. Standard operating procedures incorporating the authorities and approvals process will need to be developed, refined, and tested on a regular basis to ensure that the correct information is available when required and that the process and procedures are suitable to conduct cyberspace operations when required. The development of secure virtual and where needed obfuscated environments in which to conduct cyberspace operations is vital and success in this domain will depend on synchronising and coordinating efforts at the strategic, operational and tactical levels.

Ultimately, success in cyberspace requires preparation and an understanding of its role in a wider military context. As the cyberspace domain evolves, commanders' must remain agile, organising cyberspace forces as required. A commitment to innovation, adaptability, and coordination across the whole of society will be essential to achieving and maintaining an advantage in the cyberspace domain.

Annexes

Annex A

DEFINITIONS AND ACRONYMS

Definitions

Advanced persistent threat (APT): A targeted cyberattack that leverages multiple tactics to gain network access and remain undetected for extended periods. (Definitive Guide to Cyber Threat Intelligence, CyberEdge Group, LLC 2021).

Attack vector: This is the route or method an adversary uses to gain unauthorised access to a CIS. Attack vectors can be delivered through a phishing email, by visiting a compromised website, or by obtaining physical access to a network which can exploit vulnerabilities in software, operating systems or network protocols.

Avenues of approach (AoA): This is a relatively unobstructed route that leads to an objective of key terrain.

Centre of Gravity (CoG): The primary source of power that provides an actor its strength, freedom of action, or will to fight.

Communication and Information Systems Operations (CISOPS): Actions taken to employ, secure, operate, and maintain CIS in a way that creates and preserves Confidentiality, Integrity, and Availability (CIA), as well as user authentication and non-repudiation. (NATO AJP 3.20 Study draft 1, Mar 2025)

Cyber attack: An act or action initiated in cyberspace to disrupt, deny, degrade, or destroy by compromising communication, information, and other electronic systems, or the information that is stored, processed, or transmitted on these systems. (NATO CCDCOE Cyber Commanders' Handbook, 2020).

Cyber defence: The means to achieve and execute defensive measures to counter cyber threats and mitigate their effects, and thus preserve and restore the security of communication, information, or other electronic systems, or the information that

is stored, processed, or transmitted in these systems (NATO Standardization Office, 2025)

Cyber effect: Effects initiated in or through cyberspace (NATO CCDCOE Cyber Commanders' Handbook, 2020).

Cyber incident: Any detected anomaly compromising or that has the potential to compromise communication, information, or other electronic systems, or the information that is stored, processed, or transmitted in these systems (NATO Standardization Office, 2025)

Cyber Prioritised Asset List (CPAL): A list of prioritised critical assets essential to the mission. They are identified through the cyberspace terrain analysis process. It is a continuous process which identifies mission vital infrastructure cyber, critical national infrastructure, and key terrain cyber

Cyber risk to mission: The likelihood (probability) that an adverse event would take place in cyberspace impacting the mission.

Cyber Threat Intelligence: Information (such as indications, tactics, techniques, procedures, behaviors, motives, adversaries, targets, vulnerabilities, courses of action, or warnings) regarding an adversary, its intentions, or actions against information technology or operational technology systems (ISAO 300-2, Automating Cyber Threat Intelligence Sharing, Version 1 ISA, April 5, 2019).

Cybersecurity: The application of security measures for the protection of communication, information, and other electronic systems, as well as the information that is stored, processed, or transmitted in these systems with respect to confidentiality, integrity, availability, authentication, and non-repudiation (NATO Standardization Office, 2025)

Cyberspace (ENISA): The time dependent set of tangible and intangible assets, which store and/or transfer electronic information.

Cyberspace (NATO): The global domain consisting of all interconnected communication, information technology, and other electronic systems and networks and their data, including those which are separated or independent, which process, store, or transmit data (NATO Standardization Office, 2025)

Cyberspace environment: The interconnected digital space where information and communication technologies facilitate interactions and activities among individuals, organisations, and systems.

Cyberspace Intelligence, Surveillance and Reconnaissance Operations (CyISR): The activities and capabilities within or through the cyberspace domain to collect data and information in order to achieve results that contribute to intelligence. (NATO Standardization Office, 2025)

Cyberspace operations: Actions in or through cyberspace intended to preserve own and friendly freedom of action in cyberspace and or to create effects to achieve military objectives. (NATO Standardization Office, 2025)

Cyberspace resilience: The overall technical and procedural ability of systems, organisations, and operations to withstand cyber incidents and, where harm is caused, to recover from it with no or acceptable impact on mission assurance or continuity (NATO Standardization Office, 2025)

Cyberspace situational awareness: (CSA). Situational awareness applied in cyberspace, including information on threats, vulnerabilities, systems, and services, their mission impacts, and resulting operational risks (NATO CCDCOE Cyber Commanders' Handbook, 2020).

Decisive condition: A decisive condition is a combination of circumstances or effects or a specific key event, critical factor, or function that, when achieved, allows commanders' to gain a marked advantage over an opponent or contribute materially to achieving an objective

Defensive Cyberspace Operations (DCO): Actions in or through cyberspace to preserve own and friendly freedom of action in cyberspace. (NATO Standardization Office, 2025)

Denial of Service (DOS): DOS is an attack which denies access to a legitimate CIS, or network resources.

Distributed Denial of Service (DDOS): is when multiple machines work together to deny access to the CIS or resource.

Domain: Sphere of interest and influence in which activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent to achieve desired effects (NATO CCDCOE Cyber Commanders' Handbook, 2020).

Effects: Are the intended outcomes of the cyberspace operations. They are most often virtual but may be physical.

Effect dimension: An analytical construct that translates actions in the engagement space into the physical, virtual, and cognitive consequences that these actions may have. (NATO Standardization Office, 2025)

Engagement space: The part of the operating environment where actions and activities are planned and conducted (NATO Standardization Office, 2025)

Information environment: The interconnected functioning of CIS, individuals and organisations within the physical, virtual, and cognitive dimensions, in which cyberspace enables their global interaction and activities.

Jus ad bellum. Refers to the conditions under which States may resort to war or to the use of armed force in general.[105]

Jus in bello: Regulates the conduct of parties engaged in an armed conflict. International humanitarian law is synonymous with jus in bello.[106]

Key Terrain-Cyberspace (KT-C): Any area (physical, logical, and social) whose seisure, retention, or disruption affords a marked advantage to either combatant (MDCO Planning Guide).

Limit of Exploitation (LoE): The limit of exploitation is a line beyond which subordinate commanders' must not exploit the success of earlier stages of an attack

Living off the land (LOTL): A fileless malware cyberattack technique where the cybercriminal uses native, legitimate tools within the victim's system to sustain and advance an attack.

Main Effort (ME): A designated subordinate unit whose mission at a given point in time is the most critical to mission success.

Mission analysis: A logical process for extracting and deducing from a superior's orders the tasks necessary to fulfill a mission. (NATO Standardization Office, 2025)

Mission assurance: Process to protect or ensure the continued function and resilience of capabilities and assets critical to the execution of mission-essential functions in any operating environment or condition (NATO Standardization Office, 2025)

104 (ICRC, 2015)
105 (ICRC, 2015)

Mission-relevant terrain (MRT-C): Areas in cyberspace that support a specific military mission or objective. It is a subset of key terrain, and MRT-C may change as the mission progresses or changes focus.

Mission-vital infrastructure (MVI-C): Assets, systems, and networks that are essential for the successful execution of military operations.

Multi-Domain Operations (MDO) NATO: The orchestration of military activities across all operational domains and environments, synchronised with non-military activities to enable the Alliance to create converging effects at the speed of relevance. (NATO Standardization Office, 2025)

Multi-Domain Operations (MDO) US Army: Multi-domain operations are the combined arms employment of joint and Army capabilities to create and exploit relative advantages that achieve objectives, defeat enemy forces, and consolidate gains on behalf of the joint force commander.

Offensive Cyberspace Operations (OCO): Actions in or through cyberspace that create effects to achieve military objectives. (NATO Standardization Office, 2025)
Payload: Is the malicious software that exploits the vulnerabilities and enables the threat actor to establish a foothold and interact with the target.

Positive Identification (PID): A PID provides the reasonable certainty that a functionally and geospatially defined entity is a valid military objective.

Procedures: Actions taken by the adversary that seek to establish the conditions to successfully conduct the cyberattack, such as a brute force attack, social engineering, or malicious software.

Resilience: The ability of a system to prepare, absorb, recover, and adapt to changing conditions.

Social Engineering: The act of deceiving an individual into revealing sensitive information, obtaining unauthorised access, or committing fraud by associating with the individual to gain confidence and trust

Supply chain attacks: Threat actors may compromise the supply chain if suppliers have vulnerabilities in their security measures. Compromised software or hardware can allow an adversary to gain unauthorised access to data and/or information, leading to data theft, manipulation, and disruption of operations

Supporting effort (SE): Cyberspace operations that support and enhance the effectiveness of military or security operations across different domains by providing assistance, resources, or capabilities to the main effort.

Whole of Society: This approach emphasises collective responsibility for cybersecurity by engaging governments, businesses, civil society, and individuals to create a culture of awareness, collaboration, and shared action.

Whole of System: This approach focuses on integrating and coordinating all components of the cybersecurity ecosystem to build a resilient and adaptive defence.

Acronyms

AoA: Avenue of Approach
AoI: Area of Interest
AoO: Area of Operation
AoR: Area of Responsibility
AI: Artificial Intelligence
ASCOPE: Areas, Structures, Capabilities, Organisations, People, Events
CCIRs: Commanders' Critical Information Requirements
CERT: Computer Emergency Response Team
CIAAN: Confidentiality, Integrity, Availability, Authentication, Non-repudiation
CIMIC: Civil Military Cooperation
CIS: Communications and Information Systems
CNI: Critical National Infrastructure
COPD: Comprehensive Operational Planning Directive
CONOPS: Concept of Operations
COWG: Cyber Operational Working Group
CPAL: Cyber Prioritised Asset List
CSF: Cybersecurity Framework
DSP: Digital Service Providers
EEFI: Essential Elements of Friendly Information
ENISA: The European Union Agency for Cybersecurity
FOA: Freedom of Action
FOM: Freedom of Movement

IGO: Intergovernmental organisation
KT–C: Key Terrain Cyber
LLMs: Large Language Models
MVI-C: Mission Vital Infrastructure Cyber
MRO: Military Response Options
MDCOA: Most Deadly COA
MLCOA: Most Likely COA
NATO CCDCOE: NATO Cooperative Cyber Defence Centre of Excellence
NIST: National Institute of Standards and Technology
NGO: Non Governmental Organisation
OPLAN: Operational Plan
PID: Positive Identification
PMESII: Political, Military, Economic, Social, Information, Infrastructure
PQC: Post-Quantum Cryptography
QKD: Quantum Key Distribution
RFI: Request for Information
ROE: Rules of Engagement
SCEPVA: Sovereign Cyber Effects Provided Voluntarily by Allies
TTPs: Tactics, Techniques, and Procedures
WoS: Whole of Society
WoSa: Whole of System

Annex B

CYBER PRIORITISED ASSET LIST (CPAL)

All assets in cyberspace cannot be protected. Therefore, assets must be identified and prioritised according to their importance to the mission and resources available. The CPAL is a list of prioritised critical assets essential to the mission. They are identified through the cyberspace terrain analysis process. It is a continuous process which identifies mission-vital infrastructure (MVI-C), critical national infrastructure (CNI), and mission-relevant terrain cyber (MRT-C). Understanding the priority, the ownership and the importance of the asset to the mission will allow planners and cyber commanders' to evaluate the response options and assign the correct resources. Some of the concepts that the CPAL contributes to are as follows.

- Helps to evaluate the severity of an incident to the mission
- Analyse the interdependencies and operational dependencies of cyberspace components
- Helps to visualise the blue cyber picture
- Supports the development of a comprehensive cyberspace situational awareness (SA)

FIGURE B-1 PROCESS TO DECIDE THE CPAL



EXAMPLE CPAL TABLE

CPAL							
No	Priority	Name	Physical Location	Description / Capabilities	Asset POC	Impact on the mission in case of cyber incident	Mitigation measures

Annex C

FUNCTIONAL AREAS AND SPECIAL ADVISORS

Functional area	Main Tasks / Responsibilites
C1	• Management of cyber operations job profiles. • Identify and address cyberspace operations workforce planning and management issues, such as recruitment, evaluation, discipline, career planning, medical readiness, professional development, and retention.
C2	• Create and update the Recognised Operational Picture to maintain situational awareness. • Implement, maintain and update physical security procedures and controlled access authorisation system. • Conducts the Cyber targeting process • Vulnerability Assessment: - Determine the cyberspace posture: Which digital means are in use and are they vulnerable or not? These means can be social media, online portals, personal electronic devices, Wi-Fi, radio networks and satellite communications. - Make sure that sufficient mitigating security controls are in place to protect weak points in the cybersecurity posture of the troops These measures include the usual domains such as personnel and physical security, but must also be extended to cyberspace (password management, controlled use of accounts and administrative rights, timely updates, availability of backups,). • Threat Assessment: Determine and analyse internal and external potential real-world threat actors through multiple sources. Assess their capabilities, limitations and intent. Describe using Indicators of behaviour for possible future planned attacks and evidence of previous attacks. • Intel gathering: - Call upon the intelligence community's assets to collect the information needed for the preparation and execution of cyberspace operations. - Provide the information and intelligence gathered through cyberspace operations to the intelligence community.

C3	• Identify, create and update the cyber prioritised asset list (CPAL). • Identify key terrain cyber (KT-C). • Contributes to the cyberspace targeting process. • Create and update a contact database with all relevant national and international actors. • Integrate cyber defence aspects into all relevant processes, include cyber considerations in operational planning. • Maintain awareness of own important enablers connected to cyberspace, and identify and list cyber dependencies for the operation. • Conduct a risk assessment of those dependencies. • Coordinate mitigation efforts with C6. • Coordinate between cyber intelligence and targeting. • De-conflict cyber battle damage assessment. • Include mission-relevant cyber aspects in the comprehensive understanding of the operational environment (CUOE). • Coordinate cyber activities within the cyberspace Area of Operations (AoA). • Coordinate update and dissemination of cyber information requirements (IRs). • Monitor force commander/cyber commanders' cyber defence plans. • Conduct cyber operational working groups (COWG).
C4	• Guarantee contractors and local supply chain security compliance by maintaining awareness of cyber vulnerabilities. Information acquired in this respect may serve as I&Ws of adversary activities. • Keep track of long supply chains, with complex critical logistics cyber vulnerabilities. • Establish reach-back function to national supply chains, be aware of whether chains have sufficient protection. • Enable flexible and expedient ordering and delivery of cyber equipment.
C5	• Integrate cyberspace operations into all relevant planning products. • Maintain a cyber risk assessment matrix. • Maintain cyber defended assets database. • Maintain business continuity planning timeline (time needed to change systems, etc.).
C6	• Make sure systems are up and running, and that they stay up and running. • Be responsible for conducting the necessary CIS Infrastructure Operations. • Maintain an overview of the status of relevant systems. • Mitigation and business continuity planning. • Information assurance, CIA. • Maintain a detailed overview of infrastructure, bandwidth, sensors, coding, etc. • Support cyber defence. • Liaise with relevant boards, and commands.

C7	• Develop the goals and objectives for cybersecurity training, education, and awareness for the different target audiences. • Evaluate the effectiveness and comprehensiveness of existing training, education and awareness programmes. • Develop new or existing awareness and training materials that are appropriate for the intended audiences. • Setup effective learning environments and classroom techniques (including cyber ranges). • Follow-up of the execution the training, education and awareness programmes. • Lessons learned: Documentation of identified lessons is important for the ability to work continuously on improving the implementation of cyber aspects
C8	• Responsible for planning, managing and controlling the budget. • Prepare and manage contracts for cyber command.
C9	• Maintain contact with key host nations (HN) authorities, international organisations (IOS) and non-governmental organisations (NGOs). • Conduct and advise on the engagement with HN authorities, IOs and NGOs. • Manage cooperation with industry partners.
C10	• Guarantee compliance with already defined processes and estimates.
C Eng	• Maintain an overview of host nation (HN) and adversary critical infrastructure. • Advise on engineering aspects of infrastructures cyberspace area of interest.
InfoOps	• Maintain the cyber-related action lists for Info Ops. • Conduct Info Ops awareness campaign addressing cyber aspects. • Coordinate Information Activities related to a cyber operation. • Advise on Info Ops response options to cyber incidents.
Press Officer	• Maintain the overview of public information over cyber-related topics. • Be aware of, and advise on, the public affairs related to cyber incidents.

Special Advisors	POLAD	• Be aware of and advise on local, national, regional and international cyber policies. • Identify gaps and develop policies, programs, and guidelines for implementation such as a cyber security strategy, supply chain security concept. • Participate in International meetings and coordination
	Legad	• Be aware of, and advise on, the application of national and international laws, regulations and policies related to cyber incidents and operations. • Propose relevant offensive cyber aspects into • ROE. • Evaluate contracts to ensure compliance with legal requirements. • Evaluate the effectiveness and efficiency of laws, regulations and policies. • Translate applicable laws and regulatory documents into policy.
	STRATCOM	• Ensure coordinated and appropriate use of strategic communications activities and capabilities in support of Alliance policies, operations and activities related to the cyberspace domain.

Annex D

REFERENCES

Ajmal A.B, S. M. (2021). Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation. *IEEE Access*, 126023-126033.

Allen, D. P. (2020). *Cyber Maneuver and Schemes of Maneuver*. Retrieved from The Cyber Defense Review: https://cyberdefensereview.army.mil/Portals/6/Documents/2020_fall_cdr/CDR%20V5N3%2006_Allen.pdf

Arghire, I. (2024, Sept). *Securityweek Network*. Retrieved from New RAMBO Attack Allows Air-Gapped Data Theft via RAM Radio Signals: https://www.securityweek.com/new-rambo-attack-allows-air-gapped-data-theft-via-ram-radio-signals/

Arik, Venables, & Ottis. (2024). *The Optimal Organisational Structure for Cyber Operations Based on Exercise Lessons*. Retrieved from European Conference on Cyber Warfare and Security. 23. 37-48. 10.34190/eccws.23.1.2244: https://www.researchgate.net/publication/381651746_The_Optimal_Organisational_Structure_for_Cyber_Operations_Based_on_Exercise_Lessons

ASD. (2025, Feb 10). *Foundations for modern defensible architecture*. Retrieved from Australian Signals Directorate: https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/modern-defensible-architecture/foundations-modern-defensible-architecture

Beecroft, N., & Gilmore, &. T. (2023). *The Advantages of "Hunt Forward" Extend Beyond the Hunt*. Retrieved from BAE Syatems: https://www.baesystems.com/en/digital/feature/the-advantages-of-hunt-forward-extend-beyond-the-hunt

Bianco, D. (2023, April 26). *The Threat Hunting Guide: Everything To Know About Hunting Cyber Threats*. Retrieved March 08, 2024, from https://www.splunk.com/en_us/blog/learn/threat-hunting.html

Bower Ian. (2024). Understanding multi-domain operations. *In-depth briefing* #77 https://chacr.org.uk/wp-content/uploads/2024/07/IDB-77-MDO.pdf.

Butchenko, M. (2024, June 11). Retrieved from NewVoice: https://nv.ua/ukr/ukraine/events/ukrajinska-rozvidka-rozkrila-svoji-hakerski-ataki-po-rf-tipi-cili-ta-dosyagnennya-novini-ukrajini-50426113.html

Canadian_Centre_for_Cybersecurity. (2024). *National Cyber Threat Assessment, ISSN 2816-9182*. Retrieved from https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf

Canadian_Centre_for_Cybersecurity. (2025). *National Cyber Threat Assesment , ISSN 2816-9174*. Retrieved from https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf

Candid Wueest, H. A. (2017). *Living off the land and fileless attack techniques*. Retrieved from ISTR: https://docs.broadcom.com/doc/istr-living-off-the-land-and-fileless-attack-techniques-en

Center, C. (2023). Retrieved from Practical training of cyber security specialists continues: https://cip.gov.ua/ua/news/kibercentr-ua30-praktichna-pidgotovka-fakhivciv-iz-kiberzakhistu-trivaye

Chipeta, C. (2025, Jan 02). *Upguard*. Retrieved from https://www.upguard.com/blog/cyber-threat-landscape

cip.gov. (2023). *Cyber Center UA30: Practical training of cyber security specialists continues*. Retrieved from https://cip.gov.ua.https://cip.gov.ua/ua/news/kibercentr-ua30-praktichna-pidgotovka-fakhivciv-iz-kiberzakhistu-trivaye

cip.gov.ua. (2024, May 03). Retrieved from Cyber operations: New goals, tools and groups: https://cip.gov.ua/ua/news/kiberoperaciyi-rf-novi-cili-instrumenti-ta-grupi-analitika-khakerskikh-atak-proti-ukrayini-za-2-pivrichchya-2023-roku

CISA. (n.d.). *Defining-insider-threats*. Retrieved from insider-threat-mitigation: https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

CISA, C. &. (2024, February 7). *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*. Retrieved March 5, 2024, from https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

CISA, C. &. (2025, 02 25). *Nation-State Cyber Actors*. Retrieved from https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors

Colonel (Ret.) Jeffrey A. Voice. (2022). *Leveraging the Ontology of the Operational Cyber Mission Stack (OCMS)*. Retrieved from https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/07_Voice.pdf?ver=3Yffna2m-5WYvC8tuphmWA%3D%3D

Crossett, C. (2019). *John Hopkins University*. Retrieved from Resilience in the Face of Cyberattacks: Cyber Resilience Guidance, Cyberattack for Military Systems: https://secwww.jhuapl.edu/techdigest/Content/techdigest/pdf/V34-N04/34-04-Crossett.pdf

Cyber Diia Platform. (2024). *A Decade in the Trenches of Cyberwarfare: Ukraine's Story of Resilience*.

Davydiuk A. (n.d.). The next generation of energy intelligence: The tactical level. https://doi.org/10.15407/emodel.46.05.050.

Department of the army. (2021). *FM3-12 CEMA*. Department of the army.

Department of the army. (2022). *FM 3 0perations*. Department of the army.

Dr_Jacob_Benjamin. (2023, Oct 30). *Building Defensible Architectures for Critical Infrastructure - DRAGOS*. Retrieved from University of North Dakota: https://engineering.und.edu/research/cyber-security/symposium/_files/docs/2023/cars_2023_jacob.pdf

Ducheine, P., van Haaster, J., & van Harskamp, R. (2017). Manoeuvring and Generating Effects in the Information Environment. *Winning Without Killing: The Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*.

EU_Commission. (2022, 11 10). *EU Policy on Cyber Defence*. Retrieved from https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf

EU_NATO. (2023). *eu-nato-joint-declaration*. Retrieved from nato.int: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/1/pdf/230110-eu-nato-joint-declaration.pdf

European Union Agency for Cybersecurity, E. (2017). *ENISA overview of cybersecurity and related terminology*. Retrieved from ENISA: https://www.enisa.europa.eu/sites/default/files/all_files/2017-09-07-ENISAoverviewOfCybersecurityAndRelatedTechnology.pdf

European Union Agency for Cybersecurity, E. (2022). *ENISA Cybersecurity Threat Landscape Methodology*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology

European Union Agency for Cybersecurity, E. (2023). *ENISA Threat Landscape 2023*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

European Union Agency for Cybersecurity, E. (2024, September 19). *ENISA Threat Landscape 2024*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Flaborea, R. S. (2024, Oct). *Medium*. Retrieved from The Cyber Kill Chain: https://anticitizenone.medium.com/the-cyber-kill-chain-984358c79628

Forces, I. D. (2024). *Cyber Defence Strategy*. Dublin: Defence Forces.

Fortninet. (2023). *What Is Threat Hunting?* Retrieved March 08, 2024, from https://www.fortinet.com/resources/cyberglossary/threat-hunting

Gunnvall Ekstorm, B. L. (2022, June). *Defining, Measuring, and Analyzing Defensibility in the Defensive Cyber Operations Context*. Retrieved from Defence Technical Information Centre: https://apps.dtic.mil/sti/pdfs/AD1184908.pdf

Hałys, P. (n.d.). *Cyberspace as a domain of operational activities and the resulting challenge*. Retrieved from Scientific Journal of the Military University of Land Forces: https://www.researchgate.net/publication/352711230_Cyberspace_as_a_domain_of_operational_activities_and_the_resulting_challenge

ICRC. (2015, 01 22). *What are jus ad bellum and jus in bello?* Retrieved from https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0

Ilca Lucian & Balan Titus. (2022). Purple Team Security Assessment of Firmware Vulnerabilities. 10.1007/978-3-030-82529-4_36.

Ilca, F. B. (2022). Purple Team Security Assessment of Firmware Vulnerabilities. *Online Engineering and Society 4.0.* -, Lecture Notes in Networks and Systems.

Information_System_Authroity. (2024). *Cybersecurity in Estonia 2024*. Retrieved from www.ria.ee/sites/default/files/documents/2024-02/Cyber-security-in-Estonia-2024.pdf

Information_System_Authroity. (2025, Feb). *Cybersecurity in Estonia 2025*. Retrieved from https://www.ria.ee/sites/default/files/documents/2025-02/Cyber-security-in-Estonia-2025.pdf

Isaac R. Porche III. (2016). *Emerging Cyber Threats and Implications*. Retrieved from RAND Office of External Affairs: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT453/RAND_CT453.pdf

J. Stinissen et al. (n.d.). A Study for Existing and Possible Rules of Engagement (NATO Cooperative Cyber Defence Centre of Excellence, 2015), p. 14.

Klimburg, A. (2012, December). *National Cyber Security Framework Manual*. Retrieved from https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/

Kott, A., & Linkov, I. (2019). *Cyber Resilience of Systems and Networks*. Springer.

Landry, A. (2023, April 27). *Cyberspace and NATO*. Retrieved from ACT: https://www.act.nato.int/article/cyberspace-and-nato/

Legg, J. (2024). *Threat Hunting and False Negatives*. SANS.

Lenaerts-Bergmans, B. (2023, Feb 21). *What Are Living off the Land (LOTL) Attacks?* Retrieved from https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/living-off-the-land-attack/

Linkov, I., & Palma-Oliveira, J. M. (2017). *Resilience and Risk, Methods and Application in Environment, Cyber and Social Domains*. Springer.

Lockheed Martin. (2023). *Gaining the advantage Applying Cyber Kill Chain® Methodology to Network Defense*. Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

Magnusson, O. (2023). Cyber Threat Emulation: Exploring the capability of implementing a framework to represent known threat actor groups from public sources with offensive vulnerability assessment tools. Chalmer Universtity of Technology / University of Gothenburg.

Maj Brian Hill. (2023). The State as a Transnational Criminal Organization: A North Korea Case Study. *Journal of Indo-Pacific Affairs, Air University Press*.

Maschmeyer L. (2024). The subversive trilemma: Why cyber operations fall short of expectations. International Security, 46(2), 51–90. https://doi.org/10.1162/isec_a_00418.

Maxam, W. P., & Davis, J. C. (2024, February 19). *An Interview Study on Third-Party Cyber Threat Hunting Processes in the U.S. Department of Homeland Security*. Retrieved 03 05, 2024, from Cornell University - arXiv: https://arxiv.org/abs/2402.12252

Ministry of Defense Ukraine. (2024, March). *mil.gov.ua*. Retrieved from initiated work on the legislative definition of the term “cyber war”: https://www.mil.gov.ua/news/2024/03/28/minoboroni-inicziyuvalo-robotu-nad-zakonodavchim-viznachennyam-ponyattya-kibervijna/

Misael & Machado, B. &. (2024, March). *Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance. Applied Sciences. 14. 2116. 10.3390/app14052116*. Retrieved from https://www.researchgate.net/publication/378709279_Resilience_in_the_Context_of_Cyber_Security_A_Review_of_the_Fundamental_Concepts_and_Relevance

Mitre ATT&CK. (2024). *ATT&CK Matrix for Enterprise*. Retrieved 03 05, 2024, from https://attack.mitre.org/

Moneva and R. Luekfeld. (2023). *Insider threats among Dutch SMEs: Nature and extent of incidents, and cyber security measures,*. Retrieved from Journal of Criminology, vol. 56, no. 4, pp. 416-440, 2023: https://asiermoneva.com/publications/2023-03-15-insider-threats-among-dutch-smes/moneva_2023_insider-threats-among-dutch-smes.pdf

Moore, D. (2018). Targeting technology: Mapping military offensive network operations. *CYCON*.

N. Kaloudi and J. Li. (2020). *The AI-Based Cyber Threat Landscape: A Survey, ACM Computing Surveys, vol. 53, no. 1, pp. 1-34, 2020*. Retrieved from https://www.researchgate.net/publication/339081899_The_AI-Based_Cyber_Threat_Landscape_A_Survey

N.C. Czajka and S. Rose. (n.d.). Cyber Threats and Defenses in Government and the Military: An Overview. *Cybersecurity Journal, vol. 10*. Retrieved from Cyber Threats and Defenses in Government and the Military: An Overview, Cybersecurity Journal, vol. 10,.

National Cyber Security Centre Ireland. (2022, June 21). *National Cyber Risk Assessment*. Retrieved from https://www.gov.ie/en/publication/5a871-national-cyber-risk-assessment-2022/

NATO. (2016). *Cyber Defence Pledge*. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO AJP 3.20 Study draft 1. (Mar 2025).

NATO Cooperative Cyber Defence Centre of Excellence. (2020). *Cyber Commanders Handbook*. Tallinn: NATO CCDCOE Publications.

NATO Cooperative Cyber Defence Centre of Excellence. (2025). *Legal Concepts*. Retrieved from Legal Concepts: https://cyberlaw.ccdcoe.org/wiki/List_of_articles#Legal_concepts

NATO Standardization Office, N. (2025). *NSO*. Retrieved from NATO Standardization Office: https://nso.nato.int/nso/home/main/home

NCSC Ireland. (2024, November). *General Election 2024 Cyber Threat Landscape*. Retrieved from National Cybersecity Centre Ireland: https://www.ncsc.gov.ie/pdfs/Election_Cyber_Threat_Landscape2024.pdf

Nguyen, D. A. (2024). ow fast does malware leveraging eternalblue propagate? The case of wannacry and notpetya. *IEEE 10th international conference on network software*. https://doi.org/10.1109/netsoft60951.2024.10588886.

NIST. (2008, September). *National Institute of Standards and Technology*. Retrieved from Technical Guide to Information Security Testing and Assessment : https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-115.pdf

Olsen, X. (2022). Enterprise Purple Teaming: An Exploratory Qualitative Study.

Pardini, D. &. (2017). *Cyber Security Governance and Management for Smart Grids in Brazilian Energy Utilities. Journal of Information Systems and Technology Management. 14. 385-400. 10.4301/s1807-1775201700*. Retrieved from https://www.researchgate.net/publication/323110259_Cyber_Security_Governance_and_Management_for_Smart_Grids_in_Brazilian_Energy_Utilities

Parliament of Ukraine. (2021, May). *On urgent measures for the cyber defense of the state*. Retrieved from https://zakon.rada.gov.ua/laws/show/446/2021#Text

Peter Keough. (2024, November). *How to Assess and Defend Against the Cyber Threat Landscape*. Retrieved from IMMUTA: https://www.immuta.com/blog/how-to-assess-and-defend-against-the-cyber-threat-landscape/

Piret Pernik. (2025). Cyber Climate Convergence. *Cyber Climate Convergence in the Caribbean conference 2025*. Aruba.

Raymond, D., Conti, G., Cross, T., & and Michael Nowatkowski, .. (2014). *Key Terrain Seeking the High Ground, 6th International Conference on Cyber Conflict*. Retrieved from CCDCOE: https://ccdcoe.org/uploads/2018/10/d2r1s8_raymondcross.pdf

rnbo.gov.ua. (2023). *We are strengthening the cyber security of the regions*. Retrieved from the NCCC held a TTX and a meeting of the National Cyber Security Cluster in Ivano-Frankivsk.: https://www.rnbo.gov.ua.https://www.rnbo.gov.ua/ua/Diialnist/6596.html

Röhrig, W., & Smeaton, C. R. (2024). *Cybersecurity and Cyber Defence in the European Untion Oppertunities, Synergies and Challenges*. Retrieved from https://eda.europa.eu/docs/default-source/documents/23-27-wolfgang-r%C3%B6hrig-and-j-p-r-smeaton-article.pdf

SANS. (2024, January 31). *Continuous Purple Teaming: A Practical Approach for Strengthening Your Offensive Capabilities*. Retrieved March 08, 2024, from https://www.sans.org/blog/continuous-purple-teaming-practical-approach-strengthening-offensive-capabilities/

Schmitt, M. (2017). Articles on State Responsibility, Art. 25. Rule 26.

Staff Joint Chiefs of. (2013). *Joint Publication 3-13*.

Steingartner, &. G. (2021). *Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model*. Retrieved from https://www.researchgate.net/publication/350619730_Threat_Defense_Cyber_Deception_Approach_and_Education_for_Resilience_in_Hybrid_Threats_Model

Steshenko, A. (2023). Automating Correlation Between Attacks and Detection in Purple Team Exercises.

Steshenko, A. (2023). *University of South-Eastern Norway, Automating Correlation Between Attacks and Detection in Purple Team Exercises*. Retrieved from https://openarchive.usn.no/usn-xmlui/handle/11250/3106732

Stratcom_COE. (2021, June). *Stratcom Centre of Excellence*. Retrieved from Stratcom Centre of Excellence: https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf

Štrucl. (2022). *Comparative study on the cyber defence of NATO Member States*. Retrieved from CCDCOE: https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf

Štrucl. (2025).

Štrucl, D. (2024). Retrieved from Cyberspace as a Domain of Operations. 10.13140/RG.2.2.27717.22242: https://www.researchgate.net/publication/376521670_Cyberspace_as_a_Domain_of_Operations

T.J. Holt, Lee, J., & Smirnova, O. (2023). *Exploring Risk Avoidance Practices Among On-Demand Cybercrime-as-Service Operations*. Retrieved from Crime & Delinquency, vol. 69, no. 2, pp. 415-438, 2023: https://journals.sagepub.com/doi/abs/10.1177/00111287221103753

Telenordics. (2024). *Nordic Digital Security 2024*, Theres no time to waste. Retrieved from Telenor nordics: https://www.telenor.se/globalassets/mediabibliotek/telenor-foretag/telenor_nordic_digital_security_2024.pdf

UK MOD. (2018). *Joint Doctrine Note 1/18 Cyber and Electromagnetic ActivitieS*. Retrieved from https://assets.publishing.service.gov.uk/media/667d6471c7f64e23420900d6/ARCHIVE-JDN_1_18_Cyber_and_electromagnetic_activities.pdf

UK_MOD. (2023). *Cyber Primer Third Edition*. Retrieved from UK MOD: https://www.gov.uk/government/publications/cyber-primer

Ukraine, M. (2024, November). *Strategies and practices for Ukraine, Europe and the world*. Retrieved from Anton Demyokhin opened the scientific and practical round table: https://mfa.gov.ua/news/anton-demohin-vidkriv-naukovo-praktichnij-kruglij-stil-kiberdiplomatiya-strategiyi-ta-praktiki-dlya-ukrayini-yevropi-ta-svitu

US Cyber Command. (2018). *Achieve and maintain cyberspace superiority: Command vision for US Cyber Command*. Retrieved from https://www.cybercom.mil

US Department of Defense. (2024). *Defense industrial base cybersecurity strategy 2024*. Retrieved from https://dodcio.defense.gov/Portals/0/Documents/Library/DIB-CS-Strategy.pdf

US_AIR_FORCE. (2021, Nov). *Air Force Doctrine Publication 3-60 - Targeting*. Retrieved from https://www.doctrine.af.mil/Doctrine-Publications/AFDP-3-60-Targeting/

US_National_Cybersecurity_Strategy. (2023, March). *US_National_Cybersecurity_Strategy*. Retrieved from https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

VanBuggenhout, E. (2024). Purple Teaming: A comprehensive and collaborative approach to cyber security. *Cyber Security: A Peer-Reviewed Journal*, 207-216.

WEF. (2025, January). *Global Cybersecurity Outlook 2025*. Retrieved from World Economic Forum's Global Cybersecurity Outlook 2025: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

Williams, B. T. (2014, April). *The joint force commander's guide to cyberspace operations*. Retrieved from National Defense University, "Joint Force Quarterly 73 (2nd Quarter, April 2014)" (2014): https://digitalcommons.ndu.edu/jfq-full-issue/41