DOCTORAL THESIS

The Planning, Development and Execution of Cyberspace Operations in the Digital Information Environment

Marko Arik

TALLINNA TEHNIKAÜLIKOOL
TALLINN UNIVERSITY OF TECHNOLOGY
TALLINN 2025

TALLINN UNIVERSITY OF TECHNOLOGY
DOCTORAL THESIS
1/2026

The Planning, Development and Execution of Cyberspace Operations in the Digital Information Environment

MARKO ARIK

TAL TECH PRESS

TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Department of Software Science
The dissertation was accepted for the defence of the Doctor of Philosophy degree (Cyberspace Operations) on 11 November 2025.

Supervisor: Tenured Associate Professor Rain Ottis
Department of Software Science
School of Information Technologies
Tallinn University of Technology
Tallinn, Estonia

Co-supervisor: Dr Adrian Nicholas Venables
Department of Software Science
School of Information Technologies
Tallinn University of Technology
Tallinn, Estonia

Opponents: Professor Benjamin Knox
Norwegian University of Science and Technology
Trondheim, Norway

Professor Agnė Brilingaitė
Vilnius University
Institute of Computer Science, Faculty of Mathematics and Informatics
Vilnius, Lithuania

Defence of the thesis: 12/01/2026, Tallinn

Declaration:
Hereby, I declare that this doctoral thesis, my original investigation and achievement, submitted for the doctoral degree at Tallinn University of Technology, has not been submitted for a doctoral or equivalent academic degree.

Marko Arik

---
signature

ISSN 2585-6898 (publication)
ISBN 978-9916-80-433-9 (publication)
ISSN 2585-6901 (PDF)
ISBN 978-9916-80-434-6 (PDF)
DOI https://doi.org/10.23658/taltech.1/2026

Arik, M. (2025). *The Planning, Development and Execution of Cyberspace Operations in the Digital Information Environment* [TalTech Press]. https://doi.org/10.23658/taltech.1/2026

TALLINNA TEHNIKAÜLIKOOL
DOKTORITÖÖ
1/2026

Küberoperatsioonide planeerimine, arendamine ja läbiviimine digitaalses infokeskkonnas

MARKO ARIK

TAL TECH
KIRJASTUS

Contents

List of Publications

The list of the author's publications[1] that served as the foundation for the thesis:

I Arik, Marko; Venables Adrian; Ottis Rain (2022). Planning Cyberspace Operations: Exercise Crossed Swords Case Study. Journal of Information Warfare, 21 (4), 67−78, https://www.jinfowar.com/subscribers/journal/volume-21-issue-4/planning-cyberspace-operations-exercise-crossed-swords-case-study, [3].

II Arik, Marko; Venables, Adrian; Ottis, Rain (2024). The Optimal Organisational Structure for Cyber Operations based on exercise lessons. European Conference on Cyber Warfare and Security (ECCWS) 2024, 37−48, http://dx.doi.org/10.34190/eccws.23.1.2244, [90].

III Arik, Marko; Lugo, Gregorio, Ricardo; Ottis, Rain; Venables, Adrian (2024). Competencies Required for the Offensive Cyber Operations Planners. HCI International 2024, 26th International Conference on Human-Computer Interaction, 20–39, https://doi.org/10.1007/978-3-031-61382-1_2, [1].

IV Arik, Marko; Lugo, Gregorio, Ricardo; Ottis, Rain; Venables, Adrian (2024). Optimising Offensive Cyber Operation Planner's Development: Exploring Tailored Training Paths and Framework Evolution. Frontiers in Computer Science-Computer Security, Digital Transformation and Cybersecurity Challenges research topic within the journal, 1456–1465, https://doi.org/10.3389/fcomp.2024.1400360, [2].

V Arik, Marko; Ottis, Rain; Venables, Adrian; Lugo, Gregorio, Ricardo (2025). Enhancing Operational Planning and Situational Awareness for Cyberspace Operations. 24th European Conference on Cyber Warfare and Security (ECCWS), 18−27, https://doi.org/10.34190/eccws.24.1.3327, [3].

VI Arik, Marko; How Do NATO Members Define Cyber Operations? (2023). HCI International 2023 – Late Breaking Posters. (8−14). SpringerLink. (Communications in Computer and Information Science; 1957), https://doi.org/10.1007/978-3-031-49212-9_2, [50].

[1] All publications have been published in international peer-reviewed journals or conference proceedings, which are considered suitable for inclusion in a TalTech PhD thesis.

Author's Contribution to the Publications

As the leading author of **Publication I**, the author examined several facets of Cyberspace Operations (CO) creation, planning, and implementation concerning Exercise Crossed Swords. CO and kinetic operations differ primarily in how they are planned and carried out at the tactical, operational, and strategic levels. To maintain operational security and continuity while making attribution more difficult, COs need to set up a highly obfuscated and dispersed technology environment. COs also require coordinated intelligence requirements, integration across several cyberspace layers (physical, logical, and cyber-persona), and extensive technical preparation. In contrast to kinetic operations, COs are frequently carried out on civilian Information Communications Technology (ICT) infrastructure, which calls for rigorous evaluation of the potential legal ramifications and collateral effects. Publication I suggests twenty enhancements to enhance strategic, operational, and tactical planning and highlights thirteen distinctions between COs and kinetic operational planning.

In **Publication II**, the author analysed NATO's (The North Atlantic Treaty Organization) Cooperative Cyber Defence Centre of Excellence (CCDCOE) cyber exercises. The author evaluated CO organisational structures, optimal cyber capabilities, collected new data, and addressed challenges guiding future NATO operations. The publication emphasised the need for optimal organisational structures in cyber exercises, requiring continuous improvements to address unique challenges and maintain practical training.

The primary and leading author of **Publication III** concentrated on defining and characterising the operational level competencies needed for Offensive Cyberspace Operations (OCO) planners. The publication offers a framework for OCO planners, emphasising the need for more development and execution due to the paucity of thorough documentation and the requirement for a more comprehensive understanding of these competencies.

In **Publication IV,** the leading author examined the job description of the OCO planner, highlighting the necessity of customised training programs and ongoing framework development. The paper emphasises the intricacies of OCO planning and the necessity of cooperation, skill enhancement, and hands-on training in CO.

As this publication's primary and leading author, he was responsible for the conception and design of the study and the development of the research questions in **Publication V**. He conducted the literature review, expert interviews, and framework analysis to identify user requirements. He proposed enhancements for operational planning, particularly for COs, and analysed the results from the CS exercise to develop frameworks that support the execution of successful cyber missions. The study confirmed critical user requirements for the Cyber Planner Tool, promoting sophisticated visualisation techniques, risk management frameworks, and automation to enhance cyber mission planning. The results emphasised the significance of interoperability, decision-support tools, and real-time data analysis in CO settings for cyber planners to evaluate threats efficiently, distribute resources, and coordinate multi-domain operations.

In **Publication VI**, the sole author conducted a methodical mapping analysis to examine the definitions and interpretations of Cyberspace Operations (CO) terminology by NATO member states. This publication thoroughly examines cyberspace activities and provides a more comprehensive overview of the types of CO-s.

Abbreviations

AJP	Allied Joint Publication
BT	Blue Team
C2	Cyber Headquarters branch for situational awareness
C3	Cyber Headquarters branch for operations
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CHQ	Cyber Headquarters
CO	Cyberspace Operations
COA	Course of Action
COM	Commander
COS	Chief of Staff
CyCOP	Cyber Common Operational Picture
CyHSA	Cyber Hybrid Situational Awareness
CySA	Cyberspace Situational Awareness
CS	Exercise Crossed Swords
DCO	Defensive Cyberspace Operations
EBO	Effects-based Operations
ICT	Information and Communications Technology
IPB	Intelligence Preparation of the Battlefield
ISR	Intelligence, Surveillance, and Reconnaissance
JDN	Joint Doctrine Note
JISR	Joint Intelligence, Surveillance, and Reconnaissance
Legad	The individual should be knowledgeable about national and international laws, regulations, and policies related to cyber incidents, propose offensive cyber aspects, evaluate contracts, evaluate effectiveness, and translate them into policy
LS	Exercise Locked Shields
MCOO	Modified Combined Obstacle Overlay
MDMP	Military Decision-Making Process
NATO	The North Atlantic Treaty Organization
NICCS	National Initiative for Cybersecurity Careers and Studies
OCO	Offensive Cyberspace Operations
ROE	Rules of Engagement
RT	Red Team
SCEPVA	Sovereign Cyber Effects Provided Voluntarily by Allies
SOP	Standard Operating Procedures
TTP	Tactics, Techniques & Procedures
WT	White Team

Terms

Doctrinal publication	Doctrinal publications are considered as governmental, official publications concerning doctrines.
Blue Team	The group is responsible for defending an enterprise's use of information systems by maintaining its security posture against a group of mock attackers. [4]
Red Team	A party imitates an adversary (in the case of information security, an intruder) in a training or testing scenario (Ibid).
White Team	A neutral third-party team judges during the exercise or testing (Ibid). Also, controlling the execution.

1 Introduction

Cyberspace has evolved into a critical operational domain alongside land, sea, air, and space, where states, organisations, and individuals operate—and where various actors, including state and non-state adversaries, compete, disrupt, and defend digital assets. In this contested digital environment, the planning and execution of Cyberspace Operations (CO) present distinct challenges, including the rapid pace of technological change, information overload, and the complexities of multinational coordination.

While extensive research has been conducted in the technical domains of cybersecurity, considerably less attention has been given to operational-level planning, decision-making frameworks, and organisational structures specific to CO. Existing literature tends to focus either on technical network defence or strategic policy discussions, leaving a gap in understanding operational-level cyberspace mission planning and execution, particularly within complex, multinational military contexts.

This thesis addresses this gap by examining the competencies required for Offensive Cyberspace Operations (OCO) planners, proposing optimal organisational structures for cyber exercises, and exploring enhancements to operational planning and situational awareness frameworks. The research is motivated by the growing operational and educational need to develop coherent, evidence-based practices for CO planners and command elements operating in the Digital Information Environment.

While this research is embedded in the context of NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) CO exercises, the challenges it addresses—such as developing operational-level competencies, optimising team structures, and enhancing situational awareness—are equally relevant to national, educational, and regional resilience initiatives. The frameworks and insights presented in this work are designed for broader applicability beyond military environments, supporting contexts such as cyber defence exercises, cybersecurity education programmes, critical infrastructure protection, public-private collaboration initiatives, and cross-border resilience-building efforts within the European Union and other civilian sectors.

This thesis introduces a new CO planning paradigm that integrates theoretical and practical developments. It uniquely combines innovative approaches to improve planning frameworks, define critical skills, and optimise organisational structures while aligning with NATO cyber doctrine. By focusing on OCO planners and operational structures within the context of CO exercises, this research examines how operational-level cyberspace operations can be more effectively planned and executed in simulated operational environments. While previous research has explored COs, this thesis adopts a more comprehensive, multi-layered approach, specifically emphasising operational-level CO planning [5], [6], [7]. By focusing on OCO planners and operational structures within the context of CO exercises, this research enhances NATO's capacity to conduct coordinated and effective cyber activities in simulated operational environments. The findings provide valuable insights for refining exercise design, operational planning practices, and capability development, thereby supporting NATO's ongoing efforts to enhance cyber defence readiness. While the findings of this study are grounded in exercise-based environments, they offer actionable insights for improving operational-level CO planning frameworks. They could inform future doctrinal discussions and capability development initiatives within NATO's cyber community.

This thesis establishes a framework for conducting COs by focusing on OCO planners' competencies, optimising cyber headquarters' organisational structure, and enhancing operational planning tools and situational awareness frameworks.

This thesis employs a mixed-methods approach to identify knowledge gaps, validate theoretical frameworks, and develop CO planning tools. It includes a systematic literature review to establish a strong theoretical foundation and a design science approach to guide tool development. Additionally, it includes multiple case studies and structured interviews to gather diverse perspectives and in-depth qualitative data, ensuring a robust analysis.

With a deliberate exclusion of Electromagnetic Warfare (EMW) and Cyber and Electromagnetic Activities (CEMA) integration, this thesis concentrates exclusively on the digital layers of cyberspace. The suggested frameworks and tools may not be immediately relevant to EMW or integrated CEMA situations because they are optimised for operational-level planning of digital OCO. By methodically addressing the operational, technical, and decision-making aspects of OCO planning, as well as organisational structures, planner competencies, and the use of CO exercises as environments for capability development, this work contributes to enhancing the effectiveness and coherence of CO planning processes. The thesis takes a comprehensive approach within this clearly defined scope. This study advances knowledge of OCO planning in the digital domain. It aligns with NATO's operational cyber doctrine, although it does not fully address the full range of multi-domain integration.

Comprehensive in this sense refers to the integration of organisational, technical, and operational aspects of operational-level planning for digital OCO, including the definition of critical planner competencies, the optimisation of operational structures, and the application of these concepts in exercise-based environments. All levels refer explicitly to the strategic, operational, and tactical levels of warfare, as described in Sub-Chapter 2.1. To ensure analytical depth within a limited operational framework, it purposefully excludes EMW and CEMA, focusing on the digital domain.

This thesis references 'Multi-Domain Operations (MDO) integration' in terms of the need for CO planners to consider the operational, strategic, and tactical implications of their actions within the broader multi-domain operational environment. However, it does not examine fully integrated, synchronised cross-domain operations involving physical domains such as land, maritime, air, space, or Electromagnetic Warfare (EMW). The CCDCOE exercises analysed in this study did not incorporate such integrated cross-domain scenarios. As such, while the study acknowledges the doctrinal imperative for MDO alignment, its focus remains on planning within the digital domain, addressing how operational-level OCO planning frameworks influence and are influenced by considerations at the strategic and tactical levels in cyberspace alone. In this context, 'MDO integration' refers to vertical integration across the levels of warfare within cyberspace operations, rather than horizontal integration across multiple physical and non-physical domains.

This research relies on CCDCOE exercises, primarily Crossed Swords (CS) and Locked Shields (LS). However, these exercises have limitations that may restrict their applicability to other OCO contexts, such as information warfare, electronic warfare, and integrated cross-domain operations. NATO nations are expanding beyond traditional cyberspace boundaries by incorporating information warfare and integrated cross-domain operations. As a result, future adjustments to planning and organisational structures may be necessary. The research on NATO cyber doctrines and tools is limited to publicly available data and unclassified sources.

This research builds on CCDCOE CO exercises to understand the environment better. While these exercises have domain-specific limitations, the research enhances multi-domain operations by providing a new OCO planning framework, validating a training model, and introducing a novel CO headquarters structure. Rather than merely extending the scope of exercises, this work adapts their insights into a broader operational framework that integrates COs with the traditional domains of land, air, maritime, and space.

This study addresses the challenges of contemporary COs and proposes a methodology to enhance NATO's effectiveness in the cyberspace domain by offering both theoretical perspectives and practical tools.

The primary aim of this thesis is to develop and validate an operational-level planning framework for OCO within the digital domain, informed by CCDCOE cyber exercises.

To achieve this, the research pursues the following specific aims:

a) **Aim 1:** To identify and analyse existing gaps in operational-level CO planning methodologies and tools through a systematic literature review and empirical data from international cyber exercises.
b) **Aim 2:** To define a competency framework for OCO planners participating in operational-level CO exercises.
c) **Aim 3:** To design and propose an optimised organisational structure for cyber headquarters, Red Teams and Blue Teams, involved in operational-level OCO.
d) **Aim 4:** To develop and validate operational planning and situational awareness tools suitable for exercise-based and operational contexts in the digital domain.

This thesis makes the following original contributions to the field of cyberspace operations research:

a) **Contribution 1:** A novel operational-level planning framework for OCO in the digital domain, addressing doctrinal, organisational, and procedural requirements.
b) **Contribution 2:** A validated competency framework for OCO planners, identifying the critical knowledge, skills, and abilities required for effective operational-level planning.
c) **Contribution 3:** An optimised cyber headquarters, Red Team and Blue Team organisational model tailored for operational-level OCO, supporting improved coordination, decision-making, and situational awareness.
d) **Contribution 4:** Validated user requirements and the development of a prototype for an operational-level CO planning tool, derived from user feedback collected during structured interviews, exercise observations, and workshop sessions.

These contributions are grounded in data from CCDCOE exercises and a mixed-methods research design and are evaluated through qualitative and quantitative validation methods as described in the methodology chapter.

The motivation for this research originates from over two decades of operational military experience, including extensive participation in COs exercises such as CS and LS. Through firsthand involvement in the planning and execution of multinational COs, the researcher observed challenges in operational planning, competency development, and the limitations of existing tools and organisational frameworks. These experiences highlighted the need for structured, evidence-based research to address capability gaps in COs. This thesis integrates both academic inquiry and practical operational insights to improve planning processes and support the development of more effective, adaptable, and competency-based practices for COs.

1.1 Problem Statement

The CCDCOE conducts CO exercises to protect the digital information environment, demonstrate cyber offence and defence, improve decision-making, and fortify alliances. These exercises analyse the effects of cyberattacks on critical infrastructure, adversary communication networks, and public opinion.

NATO's CO exercises serve as critical enablers for capability development, doctrinal validation, and operational readiness in the Alliance's digital operational environment. Providing structured venues for testing cyber defence processes, frameworks, and multinational coordination. The lessons identified and operational insights gained from NATO's CO exercises play a key role in enhancing the Alliance's ability to safeguard and manage the digital information environment.

Within the context of these exercises, participants are typically organised into three primary types of teams:

Red Teams: simulate an adversary conducting cyberattacks against designated targets.

Blue Teams: act as network defenders responsible for protecting and maintaining assigned systems and services.

Cyber Command Headquarters (CHQ) Teams: serve as operational-level command and control elements, tasked with coordinating CO, planning offensive actions, and managing the operational environment.

The most relevant exercises for this research are LS and CS [8], [9]. LS, organised by the NATO CCDCOE, is the world's largest and most advanced live-fire cyber defence exercise, focused on defensive operations in a simulated crisis environment. CS is a technically advanced red-teaming and offensive cyber exercise that tests operational-level planning and coordination in a controlled yet dynamic environment [9]. These exercises directly informed the case studies, data collection, and tool development conducted in this thesis.

Military cyber exercises enhance decision-making, strengthen alliances, coordinate across domains, train personnel in both offensive and defensive cyberspace operations, and simulate information warfare scenarios—with participation from land forces, sailors, airmen, and space operators alike. Furthermore, cyber exercises are essential for NATO's success, as they establish trust, which necessitates organisational and leadership cultures [10]. In the information environment, NATO's CO exercises accomplish several goals, including modelling information warfare, educating people in cyber offence and defence, coordinating across domains, improving decision-making, and enhancing alliances. NATO CCDCOE emphasises the need for effective cyber exercise coordination and the need for leaders to understand the implications of cyber defence, aligning with NATO 2030 and preparing for emerging challenges (Ibid).

One of NATO's key challenges is the shortage of competent cyberspace operations planners, which has been highlighted in NATO-specific analyses and exercises [11], [12]. More broadly, the global cybersecurity workforce continues to face a significant shortfall, with over four million unfilled positions worldwide, which also impacts the availability of personnel suitable for military cyber roles [13], [14].

The lack of planners originates from the growth of cyber commands, branches, or services within their armed forces, which have shown a growing interest in OCO. The expansion of CO capabilities has accelerated this requirement, without the necessary training being in place [15], [16], [17]. NATO requires staff officers and civilian personnel with technical expertise in cyberspace to develop a deep understanding of how COs

contribute to NATO's overall success [18]. This research aims to develop a framework for the competencies required for OCO planning.

The lack of standardised cybersecurity terminology, especially in multidisciplinary and international contexts, poses challenges to building common competency frameworks and may hinder effective training and mission coordination [19], [20].

The operational-level CO structure faces a significant issue due to a need for better-defined and adaptive organisational structures [21], [22]. This resource gap in cyber headquarters development hinders the improvement of appropriate competencies for COs. The uncharted competencies of operational-level cyber planners and the prevailing structure of Cyber Headquarters (CHQs), which serve as a training audience in the Crossed Swords exercise, often struggle to keep up with the demands of evolving COs. Lastly, keeping a realistic perspective of the CO operational domain requires an organised planning structure inside the logical layer. With a specific focus on logical layer enhancements, this research attempts to improve the operational-level planning process for COs. Cyberspace can be described in terms of three interrelated layers: physical network, logical network, and cyber-persona (see Figure 1) to assist in the planning and execution of CO. Each layer represents a different focus from which CO may be planned, conducted, and assessed [23].

The logical network layer is a layer in cyberspace that abstracts elements from the physical network. It represents individual links, nodes, and distributed elements of cyberspace, such as data, applications, and network processes. Cyberspace capabilities, such as devices or computer programs, engage logical layer targets by creating effects in or through cyberspace (Ibid).

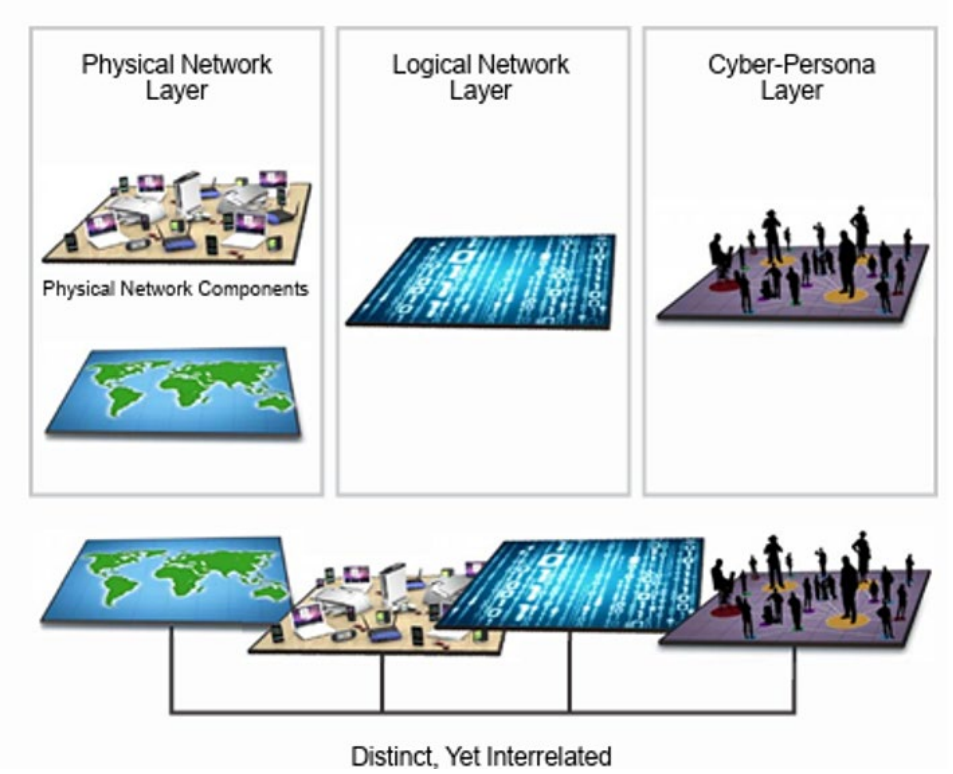

Figure 1. AJP 3-12 The Three Interrelated Layers of Cyberspace [24].

Research on enhancing operational-level cyber planning increasingly recognises the importance of adopting a layered understanding of cyberspace. As introduced in doctrinal frameworks such as U.S. Joint Publication (JP) 3-12, Cyberspace Operations, and NATO Allied Joint Publication (AJP) 3.20, Allied Joint Doctrine for Cyberspace Operations [24], [25]. Both frameworks describe cyberspace as comprising three interrelated layers: the physical, logical, and cyber persona layers, each posing distinct challenges for military operations. However, persistent challenges associated with achieving situational awareness and operational coherence within the logical layer remain underrepresented in operational doctrine and planning frameworks. Unlike the physical layer, where infrastructure is tangible and geographically fixed, or the cyber persona layer, where entities are tied to identifiable human operators, the logical layer's abstract, dynamic, and anonymised nature complicates attribution, operational synchronisation, and mission assurance. It is within this layer that offensive cyberspace effects are most often planned, delivered, and contested, making it a primary arena for adversarial exploitation and operational uncertainty.

While existing planning methodologies, such as the Military Decision-Making Process (MDMP), provide broad procedural guidance for COs, they do not offer granular operational frameworks tailored to address the distinct characteristics and vulnerabilities of the logical layer. This thesis addresses that gap by developing a set of operational-level frameworks and planning enhancements that focus on improving situational awareness, decision support, and operational synchronisation, specifically within the logical layer, particularly in the context of NATO's exercise environment.

This thesis focuses specifically on the logical layer because it represents the functional core where data is transmitted, managed, and manipulated across interconnected networks. Operational planning challenges in this layer are particularly acute due to its dynamic, concealed, and often anonymised nature, which complicates attribution, persistent access, and operational synchronisation. Unlike the physical layer, where network infrastructure and hardware can be geographically located and targeted, or the cyber persona layer, where operations focus on user accounts and identities, the logical layer's intangible, virtualised infrastructure is continuously evolving, distributed, and lacks a persistent physical manifestation. This makes it the primary arena where vulnerabilities are exploited, and effects are delivered in OCO. Therefore, a well-structured planning approach that explicitly integrates logical-layer situational awareness considerations is essential for achieving operational coherence, operational risk management, and timely decision-making during COs.

Cyberspace has become a critical domain for military operations; however, operational-level planning for OCO remains underdeveloped [26]. In particular, the complexities of the logical layer—a virtual, dynamic, and distributed environment responsible for data transmission and management—pose unique challenges that current doctrinal frameworks do not fully address. Additionally, there is a notable gap in optimising command structures, preparatory training, and competency development for operational-level planners within NATO's exercise environment.

Without a tailored framework that accounts for the operational complications of the logical layer, defines essential planner competencies, and incorporates organisational adaptability and capability development, NATO's ability to conduct and command effective COs will remain constrained. This thesis, therefore, seeks to address these gaps by developing operational-level planning frameworks, refined CO terminology, and

optimised command and training structures, specifically for the logical layer in NATO cyber exercises.

Despite NATO's growing reliance on CO for collective defence and deterrence, a lack of consensus remains regarding core definitions, operational planning processes, required competencies, organisational structures, and tools to effectively conduct and manage OCO in multinational exercises and real-world scenarios. This fragmented understanding and inconsistent preparation impair decision-making, operational effectiveness, and mission success in coalition cyber environments.

NATO CCDCOE exercises form the empirical foundation for this research, particularly LS and *C*S. These exercises involve structured roles for Red Teams (attackers), Blue Teams (defenders), White Teams (exercise control and evaluation), and Cyber Headquarters (planning and coordination). LS primarily focuses on large-scale defensive operations and strategic decision-making under cyber pressure. At the same time, CS is more tailored toward operational-level planning, OCOs, and red-team tactics. This distinction is central to how research questions in this thesis are framed and answered.

1.2 Research Questions

The primary research question of this thesis is: **How can CO be planned, developed, and executed in the Digital Information Environment?** To answer this question, the research is divided into three questions, which are divided into sub-questions to assist with their clarification and provide more detailed responses. Table 1 shows the organisation and flow of the investigation by connecting these research topics to relevant publications and thesis chapters.

RQ1: What competencies are required for the OCO planners?
1.1 What defines the role of an operational-level OCO planner?
1.2 What operational skills, digital skills, soft skills, and experience are required for the competencies needed at the operational level of an OCO planner?
1.3 What framework, including a training plan, skillset, and required competencies, is necessary to develop a competent OCO planner?

A systematic literature review, combined with qualitative expert interviews and analysis of existing training frameworks, was used to define the competencies and construct a tailored competency framework for operational-level OCO planners.

RQ2: What should the optimal organisational structure be for CO?

While this thesis focuses on OCO planning challenges, the operational environment for OCO exercises necessarily involves integrated CO structures, including defensive and command elements. Therefore, RQ2 examines optimal organisational structures for Red, Blue, and Cyber Command Headquarters teams within the broader CO exercise context, as these structures directly impact the planning, coordination, and execution of simulated OCO activities.

2.1 What is the optimal organisational structure for Red Teams in training and exercise settings?

In this context, Red Teams simulate an adversary conducting simulated attacks to test and improve the defence mechanisms of Blue Teams within a controlled training or testing environment. It is essential to distinguish this from OCO teams that perform real-world cyber missions, where factors such as the risk of loss of life and geopolitical

implications play a significant role. This research primarily focuses on organising Red Teams in training and exercise contexts, where such risks are minimised.

This research considers factors such as task specialisation, coordination efficiency, adaptability to different attack scenarios, and resource allocation when assessing the optimal Red Team structure. The goal is to identify a structure that maximises operational effectiveness, enhances learning outcomes for Blue Teams, and ensures efficient use of personnel and expertise. However, the findings are based on controlled exercise settings and may not fully translate to real-world OCO missions, where additional complexities arise.

2.2 What is the optimal Organisational Structure for Blue Teams?

Blue Teams are the training audience responsible for defending networks and systems against simulated attacks. The research examines how to organise Blue Team organisation to optimise their effectiveness during cyber exercises and training scenarios.

2.3 What is the optimal organisational structure for the Cyber Command Headquarters when acting as a training audience?

This question focuses on the structure of Cyber Command Headquarters (CHQs) when they participate as a training audience in cyber exercises, such as the Crossed Swords exercise. The research explores how to organise CHQs to support effective decision-making, coordination, and operational planning during exercises, emphasising training and educational outcomes rather than real-world mission execution.

A qualitative, comparative case study approach was employed, drawing from observations and after-action reports from NATO CCDCOE CS and LS exercises. Structured interviews with Red, Blue, and HQ team leads further refined recommendations.

RQ3: How can operational planning and situational awareness for cyberspace operations be enhanced?

3.1 What essential layers are involved in planning cyberspace operations, and how do they contribute to effective cyber mission execution?

3.2 How can operational visualisation tools enhance cyber situational awareness in CO?

3.3 What are the user requirements for a CO Planning Tool?

RQ3 was addressed by developing a conceptual operational-level OCO planning framework, integrating findings from RQ1 and RQ2. Additionally, iterative prototyping of a planning and situational awareness tool was carried out using a design science methodology. User requirements were gathered through expert interviews, exercise observations, and a prototype evaluation in a controlled exercise environment.

The research questions collectively shape the foundation of this thesis. Each RQ is addressed using a combination of systematic literature review, qualitative interviews, case study analysis, and design science-based tool development. Together, these methodologies support the construction and empirical validation of a conceptual operational-level OCO planning framework—a core contribution of this thesis.

Table 1. Research questions and thesis chapters.

Research questions	**Publications**	**Chapter 4 Sections**
Q1 What competencies are required for the OCO planners?	Publication I (context), III, IV	Chapter 4.1
1.1 What defines the role of an operational-level OCO planner?	Publication III	Chapter 4.1.1
1.2 What operational skills, digital skills, soft skills, and experience are required for the competencies needed at the operational level of an OCO planner?	Publication III	Chapter 4.1.2,4.2
1.3 What framework, including a training plan, skillset, and required competencies, is necessary to develop a competent OCO planner?	Publication III, IV	Chapter 4.1.3
Q2 What should the *o*ptimal *o*rganisational *s*tructure be for CO?	Publication I (context), II	Chapter 4.3
2.1 What is the optimal organisational structure for Red Teams?	Publication II	Chapter 4.3.1
2.2 What is the optimal organisational structure for Blue Teams?	Publication II	Chapter 4.3.2
2.3 What is the optimal organisational structure for a Cyber Command headquarters?	Publication II	Chapter 4.3
Q3 How can operational planning and situational awareness for cyberspace operations be enhanced?	Publication I (context), V	Chapter 4.4
3.1 What are the critical layers involved in cyberspace operations planning, and how do they contribute to effective cyber mission execution?	Publication V	Chapter 4.4.1
3.2 How can operational visualisation tools enhance cyber situational awareness in CO?	Publication V	Chapter 4.4.2
3.3 What are the user requirements for the CO Planning Tool?	Publication V	Chapter 4.4.3

To contextualise how this thesis addresses its research questions, Table 2 below summarises the key findings from each publication and identifies the corresponding research questions they inform. This clarifies the cumulative contribution of the publications to the overarching research objectives and highlights how foundational work on terminology and doctrinal alignment (Publication VI) supports the later operational, organisational, and tool development findings.

Table 2. Key Findings from Publications and Their Relation to Research Questions.

Publication	Key Findings	Related Research Question(s)
Publication I	Identified critical operational differences between land-based military operations and COs in exercises, highlighting unique planning, situational awareness, and command challenges specific to OCO contexts.	Motivated RQ1, RQ2, RQ3
Publication II	Proposed optimal organisational structures for Red Teams, Blue Teams, and Cyber Command Headquarters in cyber exercises, recommending task specialisation, coordination improvements, and decision-support mechanisms.	RQ2: 2.1, 2.2, 2.3
Publication III	Defined the role of operational-level OCO planners, identified required operational, digital, and soft skills, and presented a competency framework for OCO planners.	RQ1: 1.1, 1.2, 1.3
Publication IV	Developed a tailored training framework and competency development model for operational-level OCO planners, incorporating exercise-based learning and skills progression pathways	RQ1: 1.3
Publication V	Highlighted persistent challenges in achieving situational awareness at the logical layer, proposed enhanced planning frameworks and operational visualisation tools, and identified user requirements for a Cyberspace Operations Planning Tool.	RQ3: 3.1, 3.2, 3.3
Publication VI	Conducted a mapping analysis of NATO member states' definitions and interpretations of Cyberspace Operations. Identified inconsistencies in terminology and recommended the establishment of a centralised NATO cyberspace terminology authority. Emphasised the operational need for standard definitions to enable effective multinational exercises and missions.	Supports RQ3: 3.1, 3.3 (terminology clarity as a prerequisite for operational planning frameworks and planning tool requirements)

1.3 Thesis Structure

This thesis consists of 6 chapters. The first chapter presents the problem statement related to CO, outlines the research questions, describes the thesis structure, and provides an overview of the associated peer-reviewed publications that form the basis of the research. The complete list of these publications is presented on page 7.

Chapter 2 provides background and related work. It begins by reviewing existing literature and prior research on COs, examining how NATO members define Cyberspace Operations, highlighting key differences between land-based military operations and COs planning in exercises, and discussing the military's recognised levels of warfare.

Chapter 3 explains the research methodology and validation approach. It details the combined qualitative, quantitative, and experimental research methods employed throughout the thesis. It describes their application across validation events, focus group discussions, expert assessments, and exercise-based studies to ensure scientific validity and operational relevance.

Chapter 4 presents the research results, addressing the three main research questions. It identifies the competencies required for OCO planners, proposes a tailored training and development framework, and recommends optimal organisational structures for conducting COs. Additionally, it explores how operational planning and situational awareness in cyberspace can be enhanced, including addressing persistent challenges at the logical layer.

Chapter 5 provides a synthesis of the research findings and discusses their contribution to the operational and academic understanding of COs. It highlights how the thesis offers practical tools and conceptual models for COs planning and proposes evidence-based recommendations for doctrine, training, and capability development within NATO's cyberspace community.

Finally, Chapter 6 summarises the conclusions drawn from the research, articulates the significance of the work in relation to existing literature, and outlines proposals for future research.

While this thesis does not strictly follow the conventional IMRaD (Introduction, Methods, Results, and Discussion) structure, its organisation has been adapted to suit the nature of the research topic and objectives. Given the exploratory and applied character of this study—combining conceptual analysis, framework development, and user requirement gathering—the Results chapter has been intentionally structured as a comprehensive and integrated section. It presents the findings from the literature review, interviews, and validation exercises, along with the proposed conceptual solutions and tools, in a consolidated format.

It is acknowledged that, in line with good practice in computer science and engineering research, this material could alternatively be organised into several dedicated chapters, each focusing on a core contribution—for example, Competency Model for OCO, Cyber Planner Tool Design, or Operational Visualisation Techniques. However, for this study, the integrated structure was chosen to maintain coherence and directly link the results to the research questions and overarching objectives. Future work or derivative publications could explore reorganising these results into more thematically focused chapters to facilitate targeted dissemination.

2 Background and Related Work

This chapter establishes the background for this study on CO in four interrelated aspects. First, it reviews how NATO and its member nations define cyberspace operations, how COs are integrated into NATO's levels of warfare, and the doctrinal approach to CO planning and execution. Second, it highlights the key differences between land-based military operations and cyberspace operations, with a particular emphasis on operational planning for cyber exercises and the role of NATO CCDCOE's flagship exercises in advancing CO practices. Third, it introduces frameworks essential for cyberspace situational awareness and operational visualisation, including the conceptual layers of cyberspace, visualisation symbols, and decision-support systems. Finally, it identifies the research gaps emerging from this literature and practical analysis, which the thesis aims to address.

This chapter establishes the background for CO in three aspects:

a) NATO's CO terminology and definitions,
b) the key differences between land-based military operations and CO planning in cyber exercises, and
c) the importance of the operational level in planning and executing operations.

These areas provide the conceptual and doctrinal foundation for identifying current gaps and challenges in CO planning and situational awareness, which are further addressed in the thesis publications.

The increasing digitalisation of critical infrastructure has introduced new vulnerabilities that can be exploited through cyberspace, which military cyber doctrines suggest will be decisive in future conflicts, thereby undermining an opponent's ability and will to fight [27].

Since NATO declared cyberspace an operational domain in 2016 [28], member states have responded by developing national doctrines and establishing cyber commands, branches, and services within their armed forces [29], [30], [31], [32], [33], [34], [35]. This has resulted in diverse terminologies and operational approaches that complicate multinational coordination.

In examining the key differences between land-based and COs in the context of exercises, the background draws on prior analysis of doctrinal and operational planning processes (see Publication I). Furthermore, the concept of levels of warfare—strategic, operational, and tactical—is outlined, with particular attention to the operational level as the crucial link between strategy and tactical actions, especially within the dynamic environment of CO [36], [37], [25].

To clarify the terminological landscape, the section on COs definitions surveys the doctrines of NATO and allied nations, highlighting variations in how key terms and operational types are applied in practice (see Publication VI). This understanding provides context for addressing the inconsistencies and operational challenges in planning and executing CO within NATO frameworks.

Although existing literature provides a foundation for understanding cyberspace operational planning and situational awareness, limitations remain in areas such as the operational-level competencies of OCO planners and the integration of decision-support tools. These gaps are further explored in this thesis, building upon earlier research contributions, which are presented and analysed in subsequent chapters.

2.1 Levels of Warfare

Continuing the examination of NATO's doctrinal framework, this section introduces the concept of levels of warfare—strategic, operational, and tactical—and discusses how these levels are applied in the cyberspace domain. Understanding how COs are planned and executed across these levels is essential for contextualising the operational-level focus of this thesis.

NATO military doctrines and frameworks focus on the Levels of Warfare and the principles of planning, including the integration of cyberspace operations [38], [36], [39], [40]. These doctrinal documents make clear the critical importance of understanding the distinct skills and competencies required at different military levels—strategic, operational, and tactical—when planning and executing COs. The strategic level focuses on situational understanding, aligning military objectives with national or multinational goals. This level requires a comprehensive knowledge of geopolitical and security environments. In contrast, the tactical level emphasises technical skills, focusing on the execution of specific engagements and the employment of units in combat [37].

The operational level, however, is identified as the critical level for planning in COs. This level serves as the bridge between strategy and tactics, where operational art comes into play. Operational art involves designing, planning, and executing operations to achieve strategic objectives. It requires not only a deep understanding of military principles but also the ability to apply creativity, experience, and judgment in linking tactical actions to broader strategic goals [36].

Focusing more on the CO operational level, the Cyber Commanders' Handbook provides guidelines to support the planning, coordination, execution and assessment of COs to commanders and operational planners [41]. One of the Cyber command tasks is to conduct offensive operations to project power in and through cyberspace by employing cyberspace capabilities. According to the Cyber Commanders' Handbook, OCO planning requires digital reconnaissance, weaponisation through code development, exploitation of delivery, system exploitation, persistence activation, command and control and finally, the desired actions on the objective (Ibid). These stages align conceptually with adversarial behaviours described in the cyber kill chain model and frameworks such as MITRE ATT&CK, which systematise adversary tactics, techniques, and procedures (TTPs) across similar operational phases [42].

Military operations are structured by established doctrines developed by nations and alliances. The military levels of planning have been defined in the Doctrine for Planning Joint Operations [36]. Similarly, these three levels of operations are defined in the UK Defence Doctrine [37]. The Levels of Warfare are defined in the Doctrine for the Armed Forces of the United States [38]. Summarised and collated Levels of Warfare are presented in Table 3.

Table 3. Levels of Warfare, Military Planning and Operations.

Level of Warfare	Key Features & Focus	Reference
Strategic	Development of strategic military objectives and tasks in support of national security strategy. Integrates multinational efforts.	Joint Publication 1
Military planning	Defines national or multinational military objectives.	Joint Pub 5-0
Levels of Operations	Integrates military capabilities across government and with allies/partners.	Joint Doctrine Publication 0-01
Key Points	Focus on high-level, long-term goals, and collaboration with international partners.	
Operational	The operational level links strategy and tactics. Focusing on the planning of operational art.	Joint Publication 1
Military planning	Connects tactical employment of forces to strategic objectives.	Joint Doctrine Publication 0-01
Levels of Operations	Focuses on the planning of operations and creating effects to achieve strategic goals.	Joint Doctrine Publication 0-01
Key Points	Requires skills, experience, creativity, and judgment to support operational art.	
Tactical	Engagements are planned and executed to achieve military objectives.	Joint Publication 1
Military planning	Employment of units in combat to achieve tactical objectives.	Joint Pub 5-0
Levels of Operations	Focus on planning and executing combat operations.	Joint Doctrine Publication 0-01
Key Points	Focuses on individual units in combat operations.	

The military doctrines and frameworks indicate that the competencies required for OCO planners at the operational level are distinct and complex. These planners must possess a unique combination of operational, digital, and soft skills to design and manage COs effectively. They must also consider multi-domain operations and various AJPSs [43]. The operational level is crucial because, at this stage, the overall design and management of COs take place, making it the focal point for achieving strategic objectives through well-coordinated tactical actions.

Various military doctrines, including NATO's Allied Joint Doctrine for the Planning of Operations (AJP-5), support this emphasis on the operational level [39]. AJP-5 outlines the planning principles and processes that guide operational-level decision-making and the production of plans and directives. Understanding and differentiating the roles and required skills at each level of warfare is essential for the successful planning and execution of COs. This thesis focuses on the significance of the operational level in the larger framework of COs. It is essential to distinguish between the operational level of war, which refers to the planning and coordinating campaigns to achieve strategic objectives, and operations as specific activities undertaken to achieve mission goals at any level of war.

2.2 Layers of Cyberspace

As part of establishing essential frameworks for cyberspace situational awareness and operational visualisation, this section introduces the conceptual model of cyberspace layers. It discusses how the physical, logical, and cyber-persona layers structure our understanding of cyberspace and how these layers impact the design of operational planning and situational awareness tools for CO. (See Publication V, for applied use in visualisation tools.)

Cyberspace is a complex, multi-dimensional environment. Boos [44] defines it across five layers: the physical network layer, which underpins cyberspace's infrastructure; the persona layer, representing users' digital identities; the cyber-persona layer, an online extension of real-world personas; the geographical layer, mapping cyberspace to physical locations; and the logical network layer, structuring connections and interactions. These layers shape cyberspace as a socio-cultural environment, influencing how communities form, represent their identities, and interact.

In COs, NATO adopts a three-layer model to define cyberspace, comprising the physical, logical, and cyber persona layers. As outlined in AJP-3.20, Allied Joint Doctrine for Cyberspace Operations, while COs primarily focus on the logical layer, it is essential to acknowledge that these operations may also incorporate elements from the physical and cyber persona layers [25]. In NATO's model, these three layers of cyberspace are interdependent yet linked, with operations in one layer affecting the others. Decision-making in this context requires understanding how actions in each layer impact overall mission objectives and the security environment. The chain of command must be transparent and responsive, integrating inputs from diverse fields ranging from technical cybersecurity to strategic communications and intelligence.

The UK's Cyber Primer divides the layers of cyberspace into six interdependent layers: social, people, persona, information, network and geographic [45]. The goal of The Cyber Primer (Third Edition) is to give defence personnel a more thorough understanding of how UK Defence engages with cyberspace and the significance of cybersecurity [45].

In NATO, some cyberspace concepts were still being experimented with. For example, there is mention of blue, grey, and red cyberspace [46]. The new, unpublished AJP 3.20 for CO proposes a seven-layer approach: cognitive, social, cyber-persona, logical, physical network, physical and geographic. A similar approach is presented in the Master's thesis, Defending Forward in Cyberspace and The Case for Transparency [47].

Another article divides Cyberspace into three layers: Near Space, Mid Space and Far Space [48]. This approach offers a chance for situational awareness, counterattacks, and resilience. Future research aims to develop a model for predicting cyber-attack effectiveness and understanding cyberspace [48]. This approach provides a structured framework that aids in enhancing situational awareness, enabling effective counterattacks, and improving resilience against cyber threats.

Furthermore, Venables proposed another cyberspace layers approach where a mission element contextualises the seven fundamental layers—geographic, infrastructure, services, physical, syntactic, semantic, and human—to characterise each medium aspect [49]. This work categorises cyberspace into seven layers, each with a mission element, providing a comprehensive model for understanding its complexities and enhancing cybersecurity and resilience management (Ibid).

However, further research is needed to identify practical tools and techniques for mapping cyberspace, as it's unclear if all aspects can be efficiently mapped and how collected information should be stored and presented [50]. This indicates the ongoing

evolution and complexity of understanding cyberspace and the need for continued research and development.

The Intelligence Preparation of the Battlefield (IPB) outlines the evaluation of the operational environment characteristics for specific missions, describes mission variables, discusses intelligence preparation of the battlefield, and promotes a common understanding of the process [51]. The global dependence on cyberspace for information exchange necessitates consideration of its inherent vulnerabilities in the IPB process, including visualising cyberspace components and threats through three layers. The Cyberspace Operational Environment (OE) is defined by considering the physical network, logical network, cyber-persona layers, staff collaboration, and reach-back assets are crucial for evaluation (Ibid).

The OE layers in the IPB are defined as follows (Ibid):

a) Physical Network Layer – The physical network layer within the area of operations is crucial for analysing friendly and threat operations. It includes threat Command and control systems, critical nodes, physical network devices, access points, and entry points, as well as measures to prevent access.
b) Logical Network Layer – The logical network layer of a threat describes its COs, population, and communication. This includes websites, logical network configurations, vulnerabilities, current activity baselines, data access, data sharing, intrusion methods, software applications, encryption techniques, and threat information portals.
c) Cyber-Persona Layer – The cyber-persona layer incorporates an organisation's cyberspace presence, usage, data consumption, hacktivist intent, network penetration, and local actors' interactions. Analysing this layer helps identify physical persons who created or used cyber-personas, and multiple users using a single cyber-persona may indicate group activity or common affiliations.

Figure 2 depicts a cyberspace operational environment from the Army Techniques Publication [52]. In this scenario, the adversary actor, Nefarious31, operates from an internet café in Erithisi. This threat actor represents a cyber-persona—a digital identity behind which an individual or group conducts operations. Nefarious31 interacts with and influences the operational environment through multiple domains, including collaboration with government institutions, manipulation of media narratives, and engagement with military entities to disseminate propaganda and recruit new members. These activities reflect the cyber-persona layer of cyberspace, where individuals or groups use digital platforms to achieve cognitive and psychological effects.

The terrain and barriers in this environment are depicted using the Modified Combined Obstacle Overlay (MCOO), which identifies logical and physical entry points critical to Nefarious31's operations. These include infrastructure nodes and systems relevant to the physical and logical layers, such as access points, communications hubs, and network routes. Figure 2 provides a layered perspective of the cyberspace battlespace, illustrating how influence operations and physical infrastructure intersect within the operational terrain.

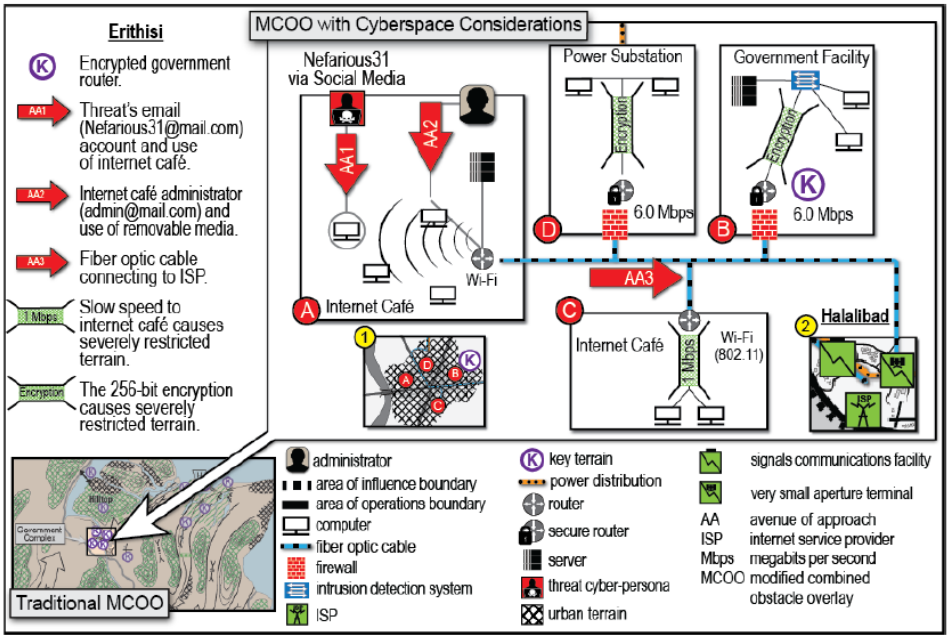

Figure 2. IPB exemplifies the Physical, Logical, and Cyber-Persona layers [52].

The IPB proposed approach provides a robust framework for CO planning at the operational level. Its technical depth, practical relevance, and holistic perspective make it well-suited for addressing the complexities of modern cyberspace environments and guiding effective operational decision-making (Ibid).

2.3 NATO and Member States' Approaches to Cyberspace Operations

This section examines how NATO and its member states define, classify, and operationalise CO. It highlights doctrinal definitions, variations in terminology and categorisation, and the frameworks used to plan and synchronise cyber and electromagnetic activities. It also establishes the specific scope of this thesis, which focuses on COs conducted in the digital information environment, particularly within the logical layer of cyberspace

2.3.1 NATO Doctrinal Framework for Cyberspace Operations

NATO defines CO as activities conducted in or through cyberspace to achieve objectives across the Alliance's operational domains. Within NATO doctrine, COs are generally categorised into three main types: Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO), and Intelligence, Surveillance, and Reconnaissance (ISR) in Cyberspace.

1) DCO focus on protecting and defending information systems and networks from cyber threats, ensuring the confidentiality, integrity, and availability of critical information assets.
2) OCO involve deliberate actions to project power in and through cyberspace, often by disrupting, degrading, or deterring adversary capabilities.
3) ISR in Cyberspace provides the intelligence and situational awareness necessary to support both DCO and OCO missions.

To coordinate COs with related operational domains, NATO has developed frameworks for synchronising cyber and electromagnetic activities. The Joint Doctrine Note (JDN) 1/18 outlines the approach to integrating cyber and electromagnetic activities (CEMA) at the operational level, ensuring coherent effects across both domains [53]. Complementary to this, Field Manual (FM) 3-12 provides guidance on integrating, synchronising, and coordinating cyberspace and electromagnetic warfare to support joint and unified land operations [54], [55]. These frameworks demonstrate NATO's recognition of the interconnected nature of cyberspace and the electromagnetic spectrum in achieving multi-domain operational effectiveness.

2.3.2 Member States' Approaches and National Variations

While NATO provides overarching definitions and frameworks, member states interpret and implement COs according to their national doctrines and strategic priorities. These variations often reflect differing organisational structures, levels of cyber capability maturity, and operational mandates.

The United States serves as a prominent example through its distinct categorisation of Department of Defense Information Network (DODIN) operations. DODIN operations focus on the management, configuration, and security of military information networks, serving as the foundation for both defensive and offensive cyberspace missions [56]. This highlights how national doctrines may expand upon or diverge from NATO's broader classifications, emphasising unique operational priorities and organisational responsibilities.

Across member states, similar differentiation can be observed in the degree of emphasis placed on DCO, OCO, and ISR functions. Some nations prioritise defensive capabilities to ensure network resilience, while others invest more heavily in offensive capacities to achieve deterrence or power projection. These national variations underscore the ongoing need for greater doctrinal harmonisation within NATO to facilitate effective joint cyber operations.

This thesis, however, narrows its focus exclusively to CO conducted within the digital information environment, particularly in the logical layer of cyberspace. It therefore excludes the electromagnetic spectrum and physical aspects of CEMA, concentrating instead on the digital and informational dimensions of CO.

2.3.3 How do NATO Members Define Cyberspace Operations

This section provides an overview of existing doctrinal approaches to CO among NATO member states. While one of the author's earlier studies explored this topic, its findings are presented here solely as background context to illustrate the current doctrinal landscape. These insights are not included in the results chapter, as they serve to frame the research problem rather than represent original findings of this thesis.

To establish a doctrinal foundation for this study, this section reviews how NATO and its member states define COs. By comparing key definitions and frameworks from NATO publications and national doctrines, this section clarifies the operational concepts that underpin NATO's approach to CO and situates this thesis within the broader doctrinal discourse.

Publication VI examines the evolving nature of national cyberspace operations. Primarily, this examines how NATO member states have developed their cyber doctrines and terminology after NATO recognised cyberspace as an operational domain in 2016 [28]. This recognition has spurred the need for a common understanding among member

states, especially as interest in OCO grows. NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn plays a crucial role in training and exercising these operations, hosting events such as the annual Exercise Crossed Swords (CS), which has evolved from technical training to include leadership, legal aspects and joint cyber-kinetic operations [9].

Over the past decade, NATO member states have proposed various cyberspace definitions but have not reached a consensus on the types of COs and concepts. "Defining cybersecurity is the first challenge in addressing the whole issue of cybersecurity law. There is no single and well-established conceptual apparatus and agreed-on definitions that would open up central terms such as "cybersecurity", "cyberdefence", or "cyber operations"" [57]. Although the preceding quote is taken from a legal source, it affirms the need for a common understanding of cyberspace operations and terminology.

NATO members should possess CO capabilities for effective interoperation with allies. However, countries have unique terminology, making it difficult to establish a unified conceptual apparatus for cyber activities [58]. Janczewski et al. presents a theoretical basis for cyber terminology, clarifying complex issues and defining key terms. He also encourages further research on cyber terms (Ibid). Additionally, NATO members lack clarity on indications and warnings of cyber threats due to a lack of established definitions and best practices in the cyber domain [18]. AJP 3.2 discusses cyberspace and COs and, as the primary NATO CO doctrine, provides definitions and guidance [25]. However, this doctrine needs an update to address emerging cyber threats and evolving operational requirements. NATO plans to update AJP 3.2 in 2025. AJP 3.2 discusses cyberspace and cyberspace operations. It should provide the necessary definitions for NATO countries as a NATO doctrine.

There are major differences in how countries define and categorise CO. According to comparative examinations of doctrinal publications from NATO member states with significant cyber capabilities, as determined by the National Cyber Power Index 2020 [59]. Although the majority of countries formally acknowledge both offensive and defensive COs, relatively few provide doctrinal definitions for cyberspace intelligence operations. Conceptual distinctions among the Allies are further highlighted by the unique doctrinal acknowledgment of Department of Defense Information Networks (DODIN) operations by the United States. A central NATO institution should be established to maintain and update a common database of cyberspace terminology and concepts, as this lack of a unified doctrinal approach has been identified as a potential source of misunderstanding during joint operations [56].

As of spring 2025, there were still discrepancies in cyberspace language, which begs the question of whether this ambiguity could discourage collaborative efforts [60]. Ambiguous terminology can cause planning, execution, and coordinated actions to be out of alignment in complex, multi-domain cyber confrontations. These difficulties could degrade NATO forces' collective cyber posture, interfere with command-and-control systems, and affect situational awareness.

2.4 Land-Based vs. Cyberspace Operations Planning in Exercises

As part of examining the conceptual and operational differences between traditional land-based military operations and COs, this section highlights the distinct characteristics of CO planning, particularly in the context of cyber exercises. It addresses how differences in the operational environment, command and control structures, and decision-making

processes necessitate adjustments in planning methodology for cyberspace operations compared to conventional military domains.

There is a growing interest within NATO in OCO for military purposes [61] [62]. NATO member states have begun integrating cyber commands within their armed forces, and by 2022, most NATO countries had established such units. In addition to conducting military activities, organisations use OCO for intelligence and cyber espionage, counterterrorism, strategic deterrence, safeguarding vital national infrastructure, and supporting alliances and partnerships [63]. OCO can remove illegal cyber infrastructures, disrupt terrorist networks, and help law enforcement target criminal groups [64]. Additionally, it can assist with strategic deterrence initiatives, provide intelligence, neutralise, or prevent cyber threats, and promote collaboration among allies [65].

The Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism requests offensive cyber effects on a target, highlighting NATO's reliance on member states for these capabilities [66].

While this thesis primarily addresses operational-level OCO planning challenges, it is essential to contextualise these within the broader landscape of military operations. Publication I contributes to the thesis by analysing key differences between traditional land-based military operations and COs planning in exercises. The findings highlight procedural, organisational, and situational awareness challenges unique to cyber exercises, particularly within the logical layer. These insights inform the problem framing and underpin the rationale for developing dedicated competencies frameworks (RQ1), optimised command structures (RQ2), and enhanced situational awareness mechanisms (RQ3). The analysis in Publication I forms part of the foundational argument for the necessity of dedicated, cyber-specific operational planning frameworks and situational awareness solutions, which are subsequently developed in this thesis.

Based on Publication I, the second aspect critically analyses vital differences between land-based military operations and COs planning in cyber exercises. These differences necessitate distinct CO planning and execution methodologies.

The Rules of Engagement (ROE) in COs must consider various legal frameworks, such as national and international laws, the UN Charter, the Law of Armed Conflict (LOAC), and human rights legislation. Because of this complexity, commanders participating in COs require precise legal frameworks and procedures [39]. For example, experts studied international law governing the use of force in cyberspace and COs during armed conflicts, creating the Tallinn Manual [67]. The publication is one of the most comprehensive analyses of COs from the international law perspective.

The CO commander’s intent may include defensive or offensive operations. If planners develop OCOs, they must align with NATO’s overarching principles and coordinate them through the SCEPVA mechanism. The lack of a centralised NATO OCO capability means member states play a crucial role in these operations [66]. In addition, the commander should link their intent with the mission, whether it is primary, enabling, supporting, or CEMA. This guidance comes from the draft of the soon to be unpublished NATO CCDCOE Cyber Commanders Handbook Version 2.

Unlike traditional military operations, COs require a dynamic and continuous intelligence-gathering process, where the time dimension plays a more critical role. In cyberspace, threats can emerge within milliseconds, necessitating real-time situational awareness and rapid decision-making. While traditional military operations also require continuous intelligence, the speed and complexity of cyber threats demand a more agile and adaptive intelligence cycle to maintain an operational advantage. Member states

provide cyber intelligence to NATO, which shares it through the Joint Intelligence, Surveillance, and Reconnaissance (JISR) system. The interconnected nature of cyberspace demands constant intelligence updating and validation to maintain situational awareness [68].

CO effects can be direct or indirect, desired, or undesired, and careful consideration of their impact on military and civilian infrastructures is required. The effects-based operations (EBO) framework is particularly relevant in COs, where targets may exist simultaneously in multiple locations, and the impact can be physical and/or logical (Ibid).

CO planning must involve detailed technical intelligence across cyberspace's physical, logical, and cyber-persona layers. This multi-layered approach ensures that all aspects of the cyber environment are considered, from hardware and software components to virtual identities [69]. The as yet unpublished draft of AJP 3.20 has changed to physical, information and virtual layers.

Wargaming is a critical component of CO planning, as it helps evaluate Courses of Action (COAs) and anticipate cyber effects. Integrating technical cyber intelligence into wargaming exercises enhances the validation of COAs and better prepares commanders for real-world scenarios [68]. Given its analytical nature, wargaming is a key tool in military and government operations planning, training, and decision-making, with its scope expanding as new concepts emerge [70]. These analytical games replicate tactical, operational, or strategic combat elements to study warfighting principles, train commanders and analysts, and assess the impact of force planning and posture decisions on campaign outcomes [71].

In the cyber domain, the vast interconnectivity and accessibility of cyberinfrastructure create opportunities for both state and non-state actors to conduct COs. Governments may leverage cybercriminals as proxy actors or mercenaries, complicating attribution and response efforts. To address these challenges, exercises such as the CCDCOE's Exercise CS serve as platforms for developing, experimenting, and validating CO planning concepts. This exercise employs structured interviews, questionnaires, and wargaming scenarios to evaluate the effectiveness of NATO's operational-level command elements and cyber specialists [9].

In Publication I, the CS 2021 revealed gaps in staff training and role definition within the Cyber Headquarters (CHQ). Only 47% of CHQ staff understood the operational environment, and many felt their roles did not align with their abilities. Recommendations included improving SOPs, adding specialised positions, and conducting frequent exercises to enhance readiness. The exercise highlighted the need for more precise mission objectives and better leadership within the CHQ. Less than half of the CHQ staff understood the operational environment, and many suggested that experienced mentors and additional training were necessary to improve mission awareness. Preparing a technical environment is critical for successful COs. This includes creating non-traceable accounts, obfuscating Information and communications technology (ICT) infrastructure, and ensuring operators have the necessary tools and resources to focus on mission objectives. The exercise emphasised the importance of deep technical planning and resource allocation to maintain operational security and achieve the desired effects.

2.5 NATO CCDCOE and its Flagship Exercises

As part of examining operational practices in CO, this section introduces the CCDCOE and its flagship cyber exercises, such as LS and CS. These exercises serve as practical environments for testing doctrinal concepts, operational planning, and situational awareness tools in realistic, federated CO scenarios. Their relevance to this study lies in their role as empirical testbeds for the approaches proposed in this thesis. (See Publications I, II and V for exercise-specific implementations.)

The CCDCOE is an accredited international organisation focused on cyber defence research, training, and exercises across technical, strategic, operational, and legal domains [72]. Among its key contributions to capability development are two flagship exercises: LS and CS, which provide the foundation for the empirical elements of this thesis.

Locked Shields is the world's largest and most complex live-fire cyber defence exercise, designed to test national cyber rapid response teams (RRTs) in defending complex IT and critical infrastructure systems under realistic cyberattack conditions [73]. Blue Teams act as national defenders, while Red Team simulates adversarial attackers. White Team serves as impartial evaluators and exercise controllers. The training scenarios involve technical defence, legal response, strategic communication, and media interaction. LS is doctrinally grounded and aimed at enhancing defensive capabilities, cross-domain coordination, and resilience under pressure [74].

Crossed Swords is a more technically focused and command-oriented exercise, with an emphasis on OCO. It aims to train military cyber planners and operators to conduct full-spectrum OCO within a realistic kill-chain framework [9]. In CS, the Red Team plays a dual role—both executing attacks and participating in offensive training objectives, often involving realistic digital twin environments and dynamic targeting tasks. The Cyber Headquarters team focuses on operational planning and coordination of offensive activities within complex scenarios.

The key distinction between the two exercises lies in their training focus: LS concentrates on defensive coordination and resilience, while CS emphasises offensive planning and execution. Both exercises contribute to the research framework developed in this dissertation by providing real-world-inspired contexts for planning tools, team structures, and competency evaluation.

2.6 Cyberspace Situational Awareness

Continuing the discussion of cyberspace operational frameworks, this section explores the concept of cyberspace situational awareness (CySA). It reviews existing definitions and models, discusses their relevance to operational planning and decision-making in CO, and highlights the specific challenges associated with maintaining situational awareness in the dynamic and opaque environment of cyberspace. (Further elaborated in Publication V).

To initiate the planning process for COs at the logical layer, it is crucial first to identify the operational area, including avenues of approach and critical terrain within the cyberspace domain.

In CO, visual planning tools are essential because they provide a unified picture of the operational environment. This makes it easier to integrate friendly and adversary assets, pinpoint weaknesses, assess risks, and aid in the creation of courses of action [75]. Additionally, by facilitating better teamwork and communication, these tools improve coordination and decision-making [76]. According to Barford et al., predictive analytics should be included in sophisticated visual tools to help operators anticipate hazards [77].

These tools ought to be able to provide data dynamically, which would improve the ability to make decisions in real-time. Network maps, for example, can show traffic flow and vulnerabilities visually, which helps with the quick detection and handling of cyber threats (Ibid).

Through the use of visual cues to depict different states, hazards, and circumstances inside the digital world, colours help people gain situational awareness in cyberspace [78]. This graphic representation accelerates decision-making and improves situational awareness. To emphasise essential topics, visual aids, including graphics, films, and tables, should be incorporated into cyberspace teaching [79], [80].

Cyberspace operational graphics aid in communicating mission-relevant information to warfighters unfamiliar with cyberspace technical details, potentially identifying physical analogies [81].

Liuyue Jiang et al.'s study emphasises the importance of user interactions in improving the effectiveness of CySA visualisations. The authors suggest better layouts and aesthetics to reduce complexity, facilitate easier sharing, and propose eight directions for future research [82]. Additionally, Franke and Brynielsson [83] emphasise the significance of incorporating human factors into cybersecurity by supporting visualisation tools that make complicated data understandable to human operators in real-time.

According to Renaud and Ophoff, CySA tools for small and medium enterprises should be in line with resource limitations and provide valuable and intuitive features that help users evaluate security information and devise reaction plans [84].

The subsequent study suggests that 3D mixed reality visualisation can enhance CySA in education and cyber threat situations. Without directly impacting decision-making processes, they emphasise the need for efficient human-to-human communication in cyber defence [85].

Understanding avenues of approach involves identifying potential routes or vectors through which cyber threats or attacks could be launched or propagated within the exercise environment. These avenues could include internet connections, network infrastructure, communication channels, and other entry points vulnerable to exploitation [52].

Key terrain in cyberspace refers to critical assets, systems, or infrastructure that are strategically important and could significantly impact mission success or security if compromised or disrupted. This could encompass vital data repositories, command and control networks, critical infrastructure components, and essential communication nodes (Ibid).

This situational awareness model builds upon earlier doctrinal constructs and enables planners to visualise the cyberspace environment in relation to friendly and adversary activity. By aligning threat vectors, communication pathways, and cyber terrain within a layered operational picture, commanders are better equipped to assess mission risks, prioritise targets, and coordinate across functional areas.

2.7 Cyberspace Symbols

Effective decision-making in CO hinges on clear, cognitively efficient visualisation of complex, dynamic information spaces. Operational planners require interfaces that present layers of cyberspace (physical, logical, cyber-persona) at appropriate levels of abstraction, support rapid pattern recognition and anomaly detection, enable interactive filtering and drill-down, and maintain consistency with established military symbology to reduce cognitive load. Human–computer interaction (HCI) literature emphasises principles

such as colour semantics, minimalism, and progressive disclosure for high-stakes visual analytics; these principles guide the symbol design and interface prototypes developed later in Publication V [3].

In support of operational visualisation for CO, this section presents an overview of the use of cyberspace-specific symbology in situational awareness tools. It discusses existing proposals, the limitations of current military symbology standards for COs, and the importance of a consistent, interoperable set of visual indicators to support decision-making during CO. This topic is applied in Publication V (Ibid).

The NATO Joint Military Symbols remain partially restricted due to their sensitive nature [86]. The APP-06 NATO Joint Military Symbology states that Cyberspace's symbol set is not fully developed, and several member states will not implement it until they are suitable. For instance, countries such as Germany, United Kingdom, and Netherlands explicitly cite the underdeveloped state of the symbology as a reason for delaying implementation. Others (e.g., ESP, FRA) suggest a cautious, phased integration, pending future system upgrades and digital tool enhancements [87].

The absence of standardised CO symbols underscores the imperative for their development and integration within existing military symbol frameworks. Standardised symbols for COs would enhance communication, coordination, and understanding among military and cybersecurity professionals, facilitating more effective response and collaboration in mission planning.

2.8 Identified Research Gaps

Drawing on the analysis in Sections 2.1–2.7, this section synthesises the key research gaps in CO doctrine, organisational structure, and situational awareness tools. These gaps form the foundation for the research questions explored in this thesis.

First, the lack of a unified doctrinal framework for cyberspace layers continues to hinder shared understanding across NATO and partner nations. Multiple models—from the three-layer construct (physical, logical, cyber-persona) [23], [51], to more complex six-layer frameworks—are used in national doctrine and academia [45], [46]. This inconsistency impairs mission planning, interoperability, and the conduct of joint operations.

Second**,** terminological divergence across NATO members complicates planning and coordination. As demonstrated in Publication VI, only some states clearly define offensive, defensive, and intelligence COs, with few aligning fully with NATO doctrinal standards [56]. The absence of common terminology can lead to misaligned expectations and operational friction in multinational contexts.

Third, there is no established competency framework for OCO planners, particularly at the operational level. While general cyber skills have been explored the role-specific requirements for OCO planning—including mission development, operational coordination, and inter-team synchronisation—remain underdeveloped [88], [89]. This gap is addressed in Publication III, which builds on lessons from the CS exercise series [7].

Fourth, Red, Blue, and CHQ team structures in NATO exercises lack empirical validation. While studies exist on penetration testing and tactical Red and Blue Teaming [90], [91], there is minimal research on organisational roles, task distribution, and command structures within CO exercises. Publication II addresses this by analysing organisational models used in LS 2022 and CS 2021–2022, based on interviews and after-action reports [92].

Fifth, situational awareness tools in CO often overlook operational planners' needs. While frameworks like Cyber Common Operational Picture (CyCOP) [93], IP-based mapping models [94], and dashboards for real-time situational awareness [95] exist, few integrate military symbology (e.g., MIL-STD-2525D), layered abstraction, or visual workflows aligned with NATO's planning doctrine [96]. Tools like Argos or the Cyberspace Effects Server illustrate the potential but lack doctrinal conformity [97], [98].

Sixth, visualisation design for CO tools remains technically focused and underexplored from an HCI perspective. Studies emphasise aesthetics, user interaction, and cognitive ergonomics [83], [84], yet practical tools often neglect usability and decision support under real-time conditions. Moreover, techniques for identifying and displaying key terrain in cyberspace remain theoretical, with limited operationalisation in planning systems [77].

Together, these gaps reveal a fragmented landscape in CO planning practice. Addressing them requires integrated research into competency frameworks, organisational structuring, and cyber planning tools—each grounded in empirical data and aligned with NATO's operational doctrine.

This chapter has established the doctrinal, conceptual, and operational foundations for COs by examining NATO definitions, levels of warfare, and the unique characteristics that distinguish COs from land-based military operations. It also introduced key frameworks for CySA and operational visualisation, including layered cyberspace models, symbolic representations, and the role of NATO CCDCOE flagship exercises in operationalising these concepts. The chapter concluded by identifying critical research gaps—particularly in situational awareness, OCO planner competencies, organisational structures, and visual planning tools—that shape the research questions and methodological approach of this thesis.

3 Methodology and validation

This chapter outlines the methodological framework employed to investigate the research questions raised in the previous chapters. Building on the doctrinal and operational context introduced in Chapter 2, it adopts a mixed-methods approach, combining systematic literature reviews, case studies, interviews, and experimental research [99]. The methodologies were chosen to suit the complex, multidisciplinary nature of COs planning and execution within NATO, ensuring practical relevance in addressing the identified research gaps. Table 4 provides an overview of the Research Questions, the Methods used to address them, and the associated Publications.

3.1 Competence Model and Definitions

To ensure terminological consistency across educational and operational contexts, the thesis adopts standard definitions of key terms based on the European e-Competence Framework [100]:
Competence: The demonstrated ability to apply knowledge, skills, and attitudes to achieve observable outcomes in specific operational contexts.
Skill: The capacity to perform tasks or activities with proficiency, often developed through practice.
Knowledge: A body of theoretical and/or factual information needed to perform tasks.
Ability: The innate or acquired cognitive or physical capability to apply knowledge and skills.
Attitude: Affective characteristics or dispositions (e.g., discipline, integrity, motivation) that influence behaviour and performance.

In this thesis, a competence is therefore treated as an integrated construct encompassing relevant skills, knowledge, and behavioural attributes needed for effective participation in cyberspace operations planning.

3.2 Research Design Overview

The research uses a mixed-methods strategy to integrate both qualitative and quantitative techniques. This choice allowed for the exploration of theoretical frameworks through systematic reviews and empirical validation via case studies, interviews, and experiments. Each method builds upon the results of the previous one, ensuring a coherent progression of knowledge and supporting triangulation of findings across research questions.

Figure 3 illustrates the sequential progression and methodological interdependence across the six core publications.

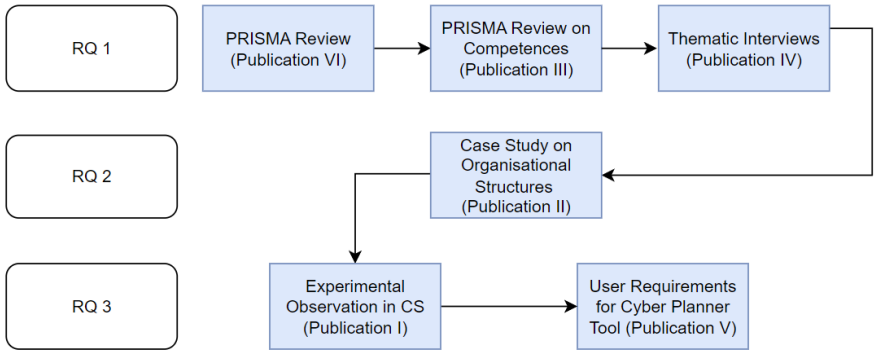

Figure 3. Sequential Methodological Flow and RQ Alignment.

Table 4. Research Questions, Methods, and Publications.

Research Question	Methodology	Type	Publications
RQ1	PRISMA Review, Case Study with Interviews	Mixed	III, IV
RQ2	Case Study, Expert Interviews	Qualitative	II
RQ3	Experimental Design, Design Science, Survey	Mixed	I, V

3.3 Methodologies per Research Question

RQ1: What competencies are required for the OCO planners?

Publication III employed the PRISMA approach to conduct a systematic review of existing knowledge on competencies required for OCO planners [101], [102]. This method ensures transparency, reproducibility, and identifies knowledge gaps. A total of 13 high-quality studies were selected using predefined inclusion/exclusion criteria (Annex 4, Table 2).

Publication IV used a qualitative case study methodology, incorporating semi-structured interviews with professionals involved in NATO-affiliated CS exercises. The interview protocol consisted of open-ended questions designed to explore how participants understand and apply various competency areas in operational settings. Questions focused on strategic decision-making, technical knowledge, team coordination, legal awareness, and communication skills. Participants were encouraged to elaborate on real-world experiences, challenges, and planning considerations.

To complement qualitative findings, a structured survey was developed. This included Likert-scale items (1–5) asking participants to rate the importance of predefined competence groups (derived from the systematic review). Participants also completed a ranking task, ordering the competence groups from most to least critical. They were required to rank all provided groups.

Survey responses were analysed using descriptive statistics. Raw ranks were normalised across all participants using the formula:

$$\text{Normalised Rank} = (Ri - \min(R)) / (\max(R) - \min(R))$$

where Ri represents the raw rank of a specific competence area. This normalization ensured comparability across differing individual ranking patterns.

The final results were visualised using a stacked horizontal bar chart, replacing the earlier pie chart, to provide a clearer, more compact overview of the comparative importance of each competence group. A new systematic diagram was also introduced to illustrate how competencies were derived from the literature and grouped into functional domains such as operational planning, legal/ethical knowledge, technical skills, and communication.

Thematic analysis of interview transcripts was conducted by multiple researchers to ensure inter-coder reliability. Emergent themes were iteratively refined and triangulated with survey findings. Methodological validity was further supported by participant transcript verification (member-checking) and alignment with established qualitative analysis frameworks [101], [102], and [103].

RQ2: What should the optimal organisational structure be for Cyberspace Operations?

Publication II used a qualitative case study approach to examine organisational structures in the LS and CS exercises. Seven expert interviews with personnel from the Estonian Defence Forces Cyber Command, NATO CCDCOE, and LS 2022 Red Team were conducted. Thematic analysis was applied to identify structural patterns and assess the effectiveness of different command configurations.

RQ3: How can operational planning and situational awareness for cyberspace operations be enhanced?

Publication I employed an experimental design to observe planning processes, coordination challenges, and tool requirements during the CS exercise [104]. These findings informed the research-led design of a Cyber Operations Planning Tool, whose user requirements were further developed and validated in Publication V.

Publication V followed the Design Science Research methodology to iteratively develop and evaluate a solution to planning challenges identified in Publication I. The Design Science Research process was aligned with the stages proposed by Peffers et al. [105]:

1) Problem Identification: Based on operational gaps observed in Publication I.
2) Objective Definition: Establishing desired planning and situational awareness capabilities.
3) Design and Development: Creating functional requirements for the Cyber Planner Tool.
4) Demonstration: Implementing the tool within a simulated NATO exercise context.
5) Evaluation: Using expert feedback and user surveys to assess functionality and usability.
6) Communication: Reporting outcomes in Publication V.

User requirements were initially derived from a combination of literature review and expert interviews. These were quantitatively validated through an international online survey targeting experienced planners who had completed NATO CCDCOE's Integrating Cyberspace Considerations into Operational Planning course. The survey, administered

via a secure platform, was analysed using descriptive statistics. A ≥70% agreement threshold was applied to confirm each requirement. A total of 22 qualified respondents from multiple NATO countries contributed diverse operational perspectives, validating the relevance and applicability of the proposed tool features.

3.4 Integration and Methodological Rationale

The methodologies were deliberately sequenced to ensure that each research output built logically upon the last:

1) Publication VI provided foundational knowledge through Kitchenham's systematic review methodology [106].
2) Publication III built on this by identifying competencies required for OCO planners through a PRISMA-based systematic review.
3) Publication IV validated these competencies through real-world application in NATO-aligned exercises using thematic interview analysis.
4) Publication II examined and compared optimal organisational structures in cyber exercises via qualitative case studies
5) Publication I observed the integration of planning challenges and cyber-kinetic operations within exercise environments, generating insights to inform solution development.
6) Publication V applied the Design Science Research methodology to develop and evaluate user requirements for a Cyberspace Operations Planning Tool. This included a demonstration in exercise settings and quantitative validation through structured surveys and expert feedback.

Throughout Publications II and IV, multiple researchers conducted thematic analysis to ensure reliability. Interview transcripts were verified through participant member-checking. In Publications I and V, prototype testing was followed by structured feedback through questionnaires and interviews, with tool performance evaluated against predefined criteria.

3.5 Summary

This chapter has rationalised the use of a mixed-methods approach and provided clarity on the sequential use of research outputs and integration of results. Systematic reviews (Publications III, VI) addressed foundational knowledge gaps for RQ1. Case studies (Publications II, IV) supplied context-specific insights for RQ2 and RQ3. Experimental research and design science (Publications I, V) facilitated the empirical development and validation of planning tools.

The following chapter presents the results derived from these methodologies, synthesising insights across systematic reviews, case studies, interviews, experimental designs, and surveys to answer the research questions.

4 Results

This chapter presents the results derived from the publications that form the foundation of this thesis. The results address the overarching research questions and their sub-questions, supporting the thesis's general objective of enhancing operational planning and situational awareness in CO. The chapter is structured around five main result areas:

1) Competencies – identifying the individual and group competencies required for effective participation in CO.
2) Training framework validation – examining the suitability of a proposed training framework for OCO planners.
3) Organisational structure – determining the optimal composition and roles within the CO planning staff.
4) Challenges in the logical layer – analysing how operational planning challenges in the logical layer of cyberspace can be addressed and mitigated.
5) Development of a Cyber Planner Tool – presenting a proposed digital tool to support operational planning and situational awareness for CO.

The chapter concludes with a consolidated synthesis of findings from these areas, mapping them back to the three principal research questions and sub-questions.

4.1 Competency Framework for OCO Planners

The impact and resources of non-kinetic capabilities, such as cyber, electromagnetic spectrum, and space-based operations, are frequently unknown to commanders. These specialist skills must be coordinated with outside units because they are not necessarily inherent to a command organisation. Building competence within headquarters components is crucial to closing this gap, ensuring that commanders can request and incorporate non-kinetic fires into joint operations, in addition to understanding their possible consequences [107]. There is now more than ever a need for enhancing training and education to include newer domains, emphasising critical thinking and problem-solving skills at commanders, delegating tasks, and trusting subordinates [108].

Addressing these challenges requires COs planners to possess a broad and sophisticated skillset that spans technical, cognitive, and managerial domains. The following sections elaborate on the competencies necessary for OCO planners, based on findings from Publications III and IV.

This section presents the findings addressing RQ1: What individual and group competencies are necessary for participating in COs? The research identified a comprehensive set of competencies essential for CO participation, based on data collected from exercise observations, participant feedback, expert interviews, and literature analysis, as documented in Publications III and IV.

The role of OCO planners demands a complex blend of skills that bridge technical expertise with operational and administrative functions. Drawing on operational task analysis, the core skill categories encompass administrative and planning, analytical assessment, communication, strategic coordination, technical cognition, critical problem-solving, and quality control. These competencies enable planners to navigate the intricate demands of cyberspace operations, effectively linking high-level strategic objectives with detailed technical execution.

Within these broad categories, two particularly critical skill subsets emerge. First, cognitive skills such as decision-making, complex problem-solving, and critical analysis are essential for managing evolving cyber scenarios and adapting plans in real-time. Second, targeting and analytical skills empower planners to identify cyber centres of gravity, optimise the use and timing of cyber weapons, and develop precise offensive plans.

Beyond technical acumen, OCO planners bring extensive expertise in ISR, Cyber Electromagnetic Activities (CEMA), and Critical Infrastructure Protection (CIP). This multi-disciplinary knowledge equips them to address challenges holistically—from gathering and analysing actionable intelligence to ensuring the resilience of vital systems.

The relative emphasis placed on various competencies reflects operational realities. The following analysis draws on findings presented later in Figure 5 (see p. 53), which illustrates the distribution of skill sets relevant to CO planning. Defensive skills constitute the largest share (35%) of a planner's focus, underscoring the persistent need to secure and stabilise systems before and after offensive actions. Offensive skills, although representing a smaller percentage (25%), require deep technical and strategic insight, which is crucial for effecting cyber attacks within the broader operational framework. Leadership (24%) and communication (16%) are woven throughout these activities, facilitating coordination, decision-making, and teamwork essential to mission success.

Importantly, this competency distribution represents the practical application and frequency of skills in daily operations rather than prescribing time allocations for individual planners. It highlights the integrated nature of leadership and communication skills as foundational elements that support both defensive and offensive tasks.

Experience and continuous professional development are central to effective OCO planning. The framework recognises that planners must combine years of military education and operational experience with ongoing training to maintain proficiency in both offensive and defensive domains. However, the literature remains sparse regarding explicit competency models for OCO planners, reflecting challenges related to classification and a lack of peer-reviewed research. This study, therefore, synthesises available knowledge, incorporating the National Initiative for Cybersecurity Careers and Studies (NICCS) framework to propose a comprehensive training and development model.

Ultimately, this section contributes a structured, evidence-based approach to defining the OCO planner role, laying the groundwork for targeted training programs within NATO and allied COs.

4.1.1 What Defines the Role of an Operational-Level OCO Planner?

Publication III explores the role of an operational-level OCO planner, analysing key responsibilities and competencies from academic, technical, and governmental literature.

According to the literature (3.1 Training Plan, 3.2 Knowledge, 3.3 Skillset and 3.4 Abilities), an operational-level OCO planner's responsibilities include organising and developing COs and emphasising offensive and defensive goals. The literature review expands on the skills of the National Initiative for Cybersecurity Careers and Studies Cyber Ops Planners, focusing on cognitive and technical aspects such as cyber intelligence analysis, targeting, and technical planning [109]. It introduces cognitive and problem-solving abilities, such as deductive reasoning and originality, and capabilities specific to COs leadership. The review also highlights hands-on expertise gained from Cyber Mission Force roles covering defensive and offensive operations. It provides insights into strategic planning, doctrine development, and joint operations, reinforcing the

argument that the literature review identifies key knowledge, skills, and experiences specific to the OCO planner role.

For example, the role of a COs Planner is defined by citing the NICE (National Initiative for Cybersecurity Education) framework [110]. These planners work with other planners, operators, and analysts to create comprehensive plans for executing or assisting the commander's mission. This entails participating in the cyber action execution process during target selection, validation, synchronisation, and integration.

Similarly, Curnutt and Sikes emphasise that a Cyber Planner's responsibilities go beyond essential tasks in the assessment process, like monitoring and planning future operations, supporting ongoing operations, and collaborating with leadership and higher headquarters [111]. This makes it clear that operational-level OCO planners have a wide range of experience in both offensive and defensive operations and mission sets. This emphasises the significance of having a broad background in cyber mission force responsibilities.

Houston makes an additional contribution by defining CO planners as experts who create and organise plans to execute offensive and defensive cyber missions [112]. This description is consistent with previous definitions but emphasises the job's analytical side.

Furthermore, according to a government contract made available by the U.S. General Services Administration, the job description includes creating briefings, translating concepts into operational tactics and procedures, and reviewing strategies, policies, and doctrines for compliance with cyberspace operations [113].

Publication III identifies a significant gap in documented competencies for OCO planners compared to defensive roles and introduces a new framework based on the NICCS Cyber Ops Planner work role. The proposed framework enhances training for Cyber Headquarters operational planners and supports NATO COs exercises by defining essential competencies, experience, and education for OCO planners.

Having established the required competencies for OCO planners, the following section evaluates how these competencies can be supported through training, using a framework validated in Publication IV.

4.1.2 Integrated Competency Framework for OCO Planners

Building on the role definition, this section integrates findings from Publications III and IV to present a consolidated view of the key competencies and experiences required for OCO planners.

Publication III examines a range of frameworks and sources that highlight the experiences, knowledge, and skills that are essential for OCO planners to answer the question (RQ 1.2), "What are the necessary digital skills, soft skills, operational skills, and experience for the competencies required at the operational level of an OCO planner?"

In Publication IV, the core question involves identifying the essential digital skills, soft skills, operational skills, and experience required for OCO planners. Several frameworks and scholarly sources are referenced to analyse and define the required competencies for operational-level OCO planners. Below is a summary of the key frameworks and sources used in the paper and their contributions to understand the skills, knowledge, and experience needed for OCO planning.

The NICCS Cyber Ops Planner Work Role outlines competencies for COs planners, including network exploitation, vulnerability analysis, and joint military operations planning [109].

The Joint Cyberspace Operations Planning (JCOP) Framework guides the integration of offensive and defensive cyberspace operations within joint military planning, emphasising the interconnection between cyberspace operations and traditional military functions (JP 3-12) [23].

NATO CCDCOE offers operational-level training in cyber defence and offence, focusing on real-world cyber incidents and simulating large-scale operations [114].

U.S. Cyber Command offers training programs on cyber threats, cryptology, intelligence collection, and full-spectrum cyberspace operations [113].

The Kill Chain Framework outlines a step-by-step process for identifying, targeting, and neutralising cyber threats. It aids OCO planners in targeting, vulnerability assessments, and integrating intelligence into mission planning [115].

RAND Corporation reports on cyber weapon procurement and shelf-life provide insights into the planning and execution of cyber-attacks [116].

The Navy Enlisted Manpower and Personnel Classifications and Occupational Standards outlines competencies for various military roles, including COs planners [117].

Based on the Publication IV dataset, Appendix 1—The Framework for Offensive Cyberspace Operations Planners specific skills were identified as follows [118]. Cyber-specific skills are essential for COs due to their technical nature and specialised knowledge. These skills include CO Assessment and Analysis, Technical Planning and Execution, Cognitive Skills Specific to COs, Cyber-Specific Decision Support, Technical Proficiency and Security, and Enterprise Information Systems Technology. Each of these skills encompass critical competencies necessary for executing COs effectively. For instance, CO Assessment and Analysis involves developing and implementing COs assessment programs, analysing network metadata, and evaluating the kill chain framework for cyber threats. Technical Planning and execution require assessing internal and external partner capabilities and tools, developing detailed CO plans, and conducting battle damage assessments and targeting analyses. Additionally, these skills support the creation of indicators of operational progress or success in cyberspace, synchronising operational assessment procedures with critical information requirements, and specialising in enterprise information systems technology.

Intangibility, technical complexity, rapid evolution, ethical and legal issues, and multi-domain integration are some of the difficulties associated with being in cyberspace. At the same time, traditional military platforms deal with observable impacts and more obvious attribution; intangible actions in cyberspace, however, demand specific forensic and intelligence analytic skills. While legal and ethical considerations are shaped by evolving international norms, technological complexity and rapid progress necessitate ongoing updates to information. For strategic impacts, multi-domain integration requires specialised coordination and synchronisation capabilities.

Operational Skills

The literature review emphasises the wide range of topic expertise and abilities needed by OCO planners. Previous studies divide cybersecurity skills into four major categories [119].

Technical Skills – These hands-on abilities are essential for operating and protecting cybersecurity systems. They include knowledge of computer networks, systems administration, cybersecurity tools, and the ability to detect and respond to cyber threats.

Managerial Skills – These skills focus on overseeing cybersecurity teams and projects. They involve strategic planning, risk management, resource allocation, and policy development to align cybersecurity efforts with broader organisational goals.

Implementation Skills – These skills pertain to the practical application of cybersecurity policies and strategies. They encompass deploying security measures, managing cybersecurity operations, and ensuring compliance with industry standards.

Soft Skills – Effective communication, teamwork, adaptability, and problem-solving abilities are critical in cybersecurity. These skills facilitate collaboration and the ability to convey technical information to non-technical stakeholders.

Although these categories apply to cybersecurity professionals in general, they also serve as a foundation for understanding the skillset required for OCO planners. The following sections explore how these skill groups translate to operational cyber warfare planning.

Skills such as targeting, battle damage assessments (BDA), and mission planning are vital for success in traditional kinetic military operations [120], [121]. However, when it comes to OCO, these same operational skills must be adapted to the unique context of cyberspace, where the "target" is often invisible, intangible, and constantly changing. While many core concepts are retained, their application in cyberspace requires new strategies, considerations, and expertise.

Critical operational abilities include targeting, battle damage assessments, and the planning and implementation of COs. According to Nizich, Bender, and Barber et al., targeting abilities are crucial [122], [122], [123], [5]. These abilities are essential for operations in cyberspace. OCO strategists must understand issues such as the law of war, the cyber centre of gravity, and the obsolescence and perishability of cyberweapons [124]. They also need to be adept at analysing network data and incorporating COs into larger-scale command plans [125]. The specific contributions of new information include the deployment and reuse periods (shelf-life) of cyberweapons and the cyber centre of gravity (a vital point—a source of strength for the adversary's cyber activities) [124].

A cyber weapon is a malicious software tool designed to disrupt computer systems, networks, or information, exploiting weaknesses in the target's cyberinfrastructure for strategic, operational, or tactical goals. These weapons can be used in OCOs for attacks like denial of service, data exfiltration, system disruption, or cyber espionage [126].

Additionally, the NICCS and the NICE Cybersecurity Workforce Framework 2.0 provide a strong emphasis on vital competencies such as operational security, intelligence analysis, and coordination of ongoing and future actions [109]. Neville et al. [127] offer a cognitive skills research methodology to describe competencies necessary for understanding cyber hazards and targeted procedures, such as cyber intelligence analysis.

Comprehending and interpreting situational awareness is an essential skill for CO planners. Enabling prompt and pertinent decision-making requires a thorough grasp of the existing circumstances. According to the US Army Field Manual, situational awareness is "knowledge and understanding of the current situation which promotes timely, relevant, and accurate assessment of friendly, enemy, and other operations within the battlespace to facilitate decision making [128]." CO planners may evaluate vulnerabilities, foresee risks, and make well-informed decisions during operations thanks to this awareness.

Digital Skills

OCO planners require digital competencies across several computing domains, including ICT, network analysis tasks (e.g., traffic monitoring and anomaly detection), and core principles of cybersecurity such as connection security, threat modelling, and risk assessment.

According to Caton [129] and Shoemaker, Kohnke, & Sigler [130], cyber planners must be educated on digital technologies, especially ICT, cybersecurity, and emerging cyber threats. Digital technology refers to electronic tools, devices, and systems that process, transmit and store data in binary form [131]. The importance of digital competencies is emphasised by Curnutt & Sikes [111] for the assessment and management of cyber activities. According to Withers et al. [132] it is critical to understand cyberspace operations and integrate cyber capabilities into more extensive operational plans.

OCO planners need to be proficient in using digital systems, assessing network metadata, and utilising technical planning tools to support operational planning [123], [127]. Due to their in-house development, customisation, and limited public access, these products are guaranteed to satisfy specific operational and security needs. A comprehensive list of examples of tools is provided in the DevSecOps Fundamentals Guidebook: DevSecOps Activities & Tools. This study lists 60 tools for enhancing security, automation, compliance, and operational efficiency [133].

The list includes methods for managing binary artefacts, asset inventory, backup, build, code quality review, compliance monitoring, configuration automation, cyber threat intelligence, data masking, database automation, security audit, and testing. It also includes tools for detecting vulnerabilities, managing bugs, logging and many others.

Soft Skills

In OCO planning, soft skills such as critical thinking, problem-solving, communication, and judgment are equally important. The Navy Personnel Command [117] lists necessary soft skills, such as critical thinking, systems analysis, communication, and coordination. These are essential for working with mission teams and leadership to reach crucial strategic decisions quickly.

Additionally, cooperation, cross-functional teamwork, and collaboration are highly valued soft skills in the NICE Workforce Framework for Cybersecurity (NIST SP 800-181 Rev 1) [134]. These soft skills are critical for executing offensive and defensive cyber missions, which often require complex team dynamics and critical decision-making.

Experience

OCO planners must have a knowledge of both offensive and defensive COs. According to Curnutt & Sikes Candidates for this role typically have experience with both offensive and defensive Cyber Mission Force responsibilities [111]. Houston asserts that CO planners require a high level of proficiency in completing assessments to carry out offensive or defensive missions effectively [112].

Additionally, Bender highlights the importance of practical training through a comprehensive curriculum designed to give OCO planners the tools they need to address the challenges of cyber warfare [123]. In line with this, the RAND Corporation emphasises the importance of civilian and military education in developing the skills needed by OCO planners [135].

Publication IV enhances the knowledge set of COs planners by providing a more specific set of competencies for operational-level OCO planners. It focuses on tactics, techniques, procedures, cyber threats, and operational planning in OCO. Publication IV

also includes knowledge of the cyber centre of gravity, cyberweapon deployment and reuse periods, and core competencies. This publication provides an overview of the information that OCO planners need to be proficient in the following areas: leadership, management, communications, offensive and defensive plans.

By emphasising cognitive skills, including deductive reasoning, inventiveness, and problem sensitivity, Publication IV improves the capabilities of Cyber Ops Planners. To effectively coordinate offensive cyber activities, it bridges the gap between general communication and cooperation skills and specialist competencies. These core competencies—operational planning, communication, technical proficiency, and ethical-legal understanding—are illustrated in Figure 4.

Figure 4 visualises the conceptual relationship among key skill domains that underpin effective OCO planning. At the top of the diagram, Operational Planning serves as the central integrative function. From this central node, a direct connection leads to Core Competencies, which branch into three critical domains: Legal and Ethical Knowledge, Technical Skills, and Communication.

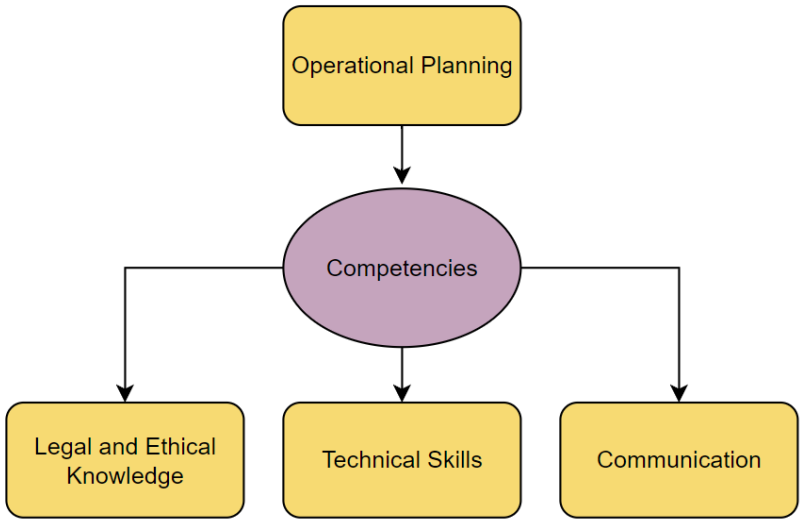

Figure 4. Relative Distribution of Core Competency Areas for OCO Planners.

This configuration illustrates how successful OCO planning depends on the interaction between these three domains. Legal and ethical knowledge ensures compliance and legitimacy in CO; technical skills provide the functional expertise required to design and execute operations; and communication competencies enable coordination, collaboration, and situational awareness across organisational and inter-agency boundaries.

Figure 4 conveys the structural interdependence of these competencies. It shows that effective operational planning in cyberspace emerges not from isolated expertise but from the alignment of technical, ethical, and communicative capabilities within a coherent planning framework.

For hiring authorities or training designers, the insight from this model is that strengthening OCO planning capacity requires balancing these domains—ensuring that planners are not only technically proficient but also capable communicators and ethically informed decision-makers.

In summary, an operational-level OCO planner must possess technical, analytical, and leadership skills and broad expertise in COs Neville et al. [127], Nizich [122] and Bender [123] define the necessary competencies in detail, including knowledge gained through formal education, practical experience in offensive and defensive cyber missions, and operational, digital, and soft skills [127], [122], [123]. An operational-level OCO planner must possess a diverse skill set, which includes technical, analytical, and leadership skills, along with a deep understanding of COs. Competencies such as extracting relevant information from complex technical details and translating it into mission-specific aspects that are easily understandable for a mission commander—and similarly, to communicate operational needs back to the technical teams—are crucial. These competencies, emphasised by frameworks and supported by various literature sources like Neville et al. [91] and Nizich [83] highlight the critical role of continuous education and training.

The research uses many questionnaire responses to ensure that the results represent a wide range of knowledge and perspectives on OCO. The experiments evaluated competencies necessary for efficient OCO planning, such as technical expertise, communication skills, teamwork, and cognitive abilities. By offering actual data on the distribution of these talents among OCO planners, these trials directly address the research questions (RQs) and validate the previously described theoretical frameworks.

The study's primary value is its capacity to map and quantify the essential skills of OCO planners, offering a thorough framework that combines operational and technical components. It also demonstrates how crucial cross-disciplinary education and ongoing training are to preserving operational efficacy.

4.1.3 Training Plan and Skill Development

Publication III offers a thorough method for creating a framework for OCO planners, including training schedules, necessary experience, skill sets and competencies. The following provides an overview of that framework, detailing the essential components needed to cultivate proficient OCO planners who can effectively navigate the complexities of OCOs.

Training Plan

The suggested training plan outlines several courses necessary for OCO planners. It should be clarified that this plan was compiled based on publicly available information during the study. There may be other courses or training paths that are not publicly known. Every course concentrates on essential topics such as:

a) National Defense University's "CAPSTONE" course emphasises joint warfighting, the security environment, and operational and strategic levels of conflict [136].
b) Information Operations Command's Basic CNO Planners Course, focusing on planning, criteria, battle damage assessment, and joint doctrine [137].
c) The Army Cyberspace Operations Planners Course prepares individuals for full-spectrum cyberspace operations (attack, ISR, defence) [138].

Table 5. Proposed OCO planner's training plan.

Course name	Description	Knowledge Areas
U.S. National Defence University "CAPSTONE" course	Explains the joint warfighting concept, security environment, conflict dynamics, and operational and strategic levels. Emphasises Allied and Partner contributions.	Joint warfighting, security environment, conflict dynamics, operational and strategic levels, Allied and Partner contributions.
U.S. Information Operations Command's Basic CNO Planners Course	Utilises case studies and scenarios for planning criteria, effects, capability choice, success/failure, collateral effects, and battle damage assessments. Based on joint doctrine and U.S. DoD tactics.	Joint warfighting, security environment, conflict dynamics, operational and strategic levels, Allied and Partner contributions.
U.S. Army Cyberspace Operations Planners Course	Prepares for planning full-spectrum cyberspace operations, including attack, ISR, defence, and integration into Army and Joint planning processes. U.S.-only students.	Full-spectrum cyberspace operations, attack, ISR, defence, and integration into planning processes.
U.S. Cyber 200/300	Provides operator's perspective on network exploitation and vulnerabilities, integrating into the joint fight against cyber threats for U.S. Armed Forces.	Network exploitation, vulnerabilities, and joint fight against cyber threats.
U.S. Cryptologic Network Warfare Specialist qualification course	Focuses on advanced capabilities in cyberspace operations, cryptology, electronic warfare, signals intelligence, and space. U.S. citizens only.	Cyberspace operations, cryptology, electronic warfare, signals intelligence, space.
U.S. Joint Network Attack Course (Cyber Capabilities Developer Officer Course)	Provides initial training in military doctrine, cyber threats, cyberspace and electromagnetic warfare operations, and electromagnetic spectrum fundamentals. U.S. citizenship is required.	Military doctrine, cyber threats, electromagnetic warfare operations, spectrum fundamentals.
U.S. Joint Advanced Cyberspace Warfare Course	Covers full-spectrum cyberspace operations, global cryptologic platforms, the intelligence community, threats, planning, and analysis. Exclusive for U.S. Cyber Command.	Full-spectrum cyberspace operations, global cryptologic platforms, intelligence community, threats, planning, and analysis.
U.S. Joint Information Operations Planners Course	Focuses on planning, integrating, and synchronising full-spectrum information operations into joint operational-level plans. Open to multinational students.	Information operations planning, integration, synchronisation, military deception, operations security, interagency coordination, and intelligence preparation.
U.S. Joint Intermediate Target Development Course	Teaches research and documentation for developing virtual targets. U.S. Joint Chiefs of Staff course.	Researching, documentation, virtual target development.

The courses listed in the training plan are U.S.-based, but they do not necessarily represent the only options for CO planners. While these courses are specific to the U.S. military and some are limited to U.S. citizens, similar training programs and courses are often offered by other NATO allies or international organizations. Each nation may have its own equivalent programs or institutions that provide similar knowledge areas, such as joint warfighting, COs, and information operations planning.

Table 4, based on Publication III, is essential for fully understanding the training required for planning COs, including the technical knowledge of network exploitation, vulnerabilities, cyber threat analysis, and operational coordination.

Skillset

The framework expands the skill set of the Cyber Ops Planners for the NICCS by including [109]:

a) Technical Skills: Analysing network metadata, assessing battle damage, and obtaining intelligence are all crucial for COs. Offensive operations are closely related to competencies such as cognitive analysis, targeting, and technological planning (cyber intelligence analysis, targeting, and analytical abilities).
b) Administrative and Managerial Skills: These are required to oversee joint operations, supervise cyber teams, and incorporate COs into more extensive military plans.
c) Soft Skills: Cooperation and coordination with other mission components require communication, problem-solving, and adaptability.

Based on Publication III, Figure 5 illustrates the skillset required of OCO planners. It encompasses seven key areas: administrative and planning, analytical and assessment, communication and presentation, strategic planning and coordination, technical and cognitive skills, critical thinking and problem-solving, and quality control and monitoring. The figure highlights how these competencies bridge the gap between administrative and operational planning activities and the technical dimensions of COs. Publication IV (Tables 10 and 12) presents job task analysis data that forms the basis of this framework, detailing the frequency and operational importance of each skill category within the context of OCO planning.

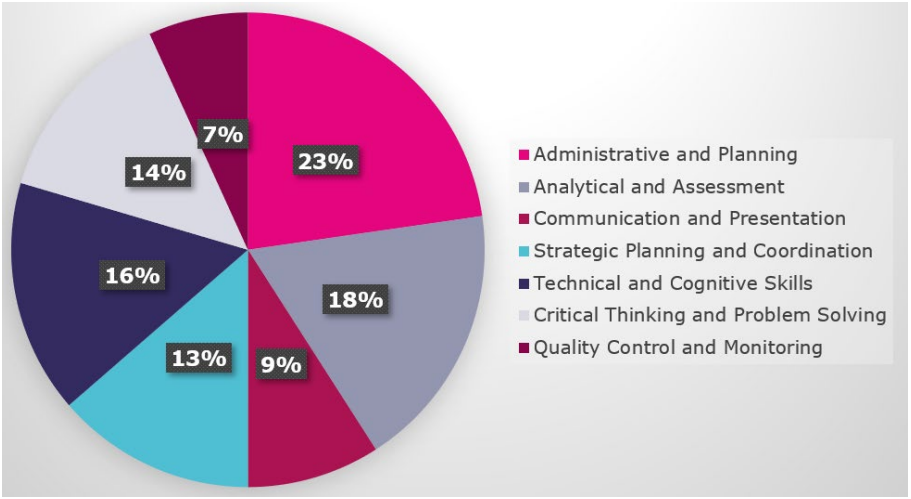

Figure 5. Key Skill Categories of OCO Planners.

Competencies

According to Publication III, the following skills are relevant to the OCO and are necessary for an OCO planner:

a) Cognitive Skills: These include decision-making, critical analysis, complicated scenario problem-solving, obsolescence management, and the deployment of cyberweapons.
b) Targeting and Analytical Skills: Developing the cyber centre of gravity, controlling the perishability and reuse of cyberweapons, and planning offensive COs require targeted analysis.

Cyber planners possess various skills because of their expertise in offensive and defensive operations. Their knowledge includes ISR, where they collect and evaluate data to assist in making decisions. They are also proficient in Cyber Electromagnetic Activities (CEMA), which allows them to combine operations in the electromagnetic spectrum and cyberspace successfully. Critical Infrastructure Protection (CIP), which guarantees the security and resilience of vital systems and assets, is another area where cyber planners excel. Their broad skill set enables them to tackle intricate problems in COs holistically. They are dedicated to lifelong learning and professional growth and are thoroughly aware of cyberspace, core competencies, professional networking, social cooperation, and ICT. Figure 6 represents the distribution of key competencies within OCO planners. Broken down into four main categories: Leadership (24%), Communications (16%), Defensive Skills (35%), and Offensive Skills (16%).

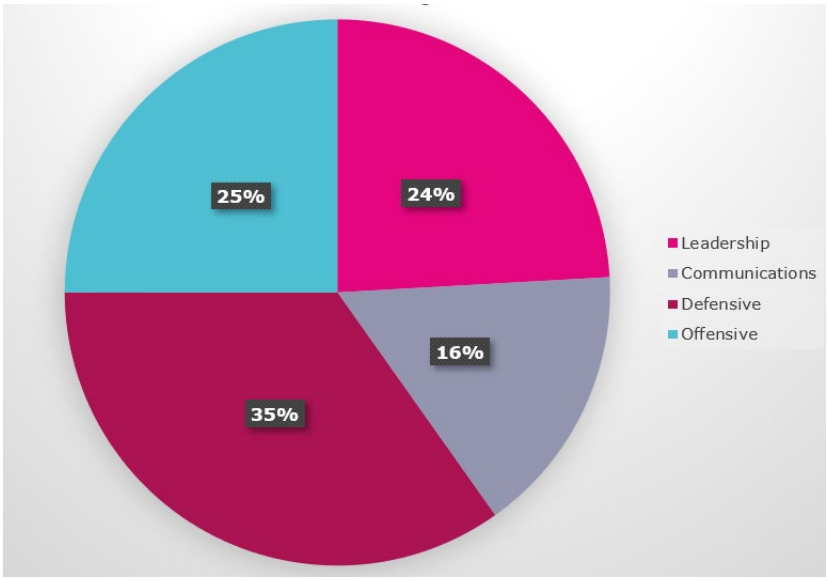

Figure 6. OCO Planning Competency Areas.

Figure 6 aims to visualise the relative weighting of competency areas observed in the operational practice of OCO planners rather than suggesting an individual planner needs to be 25% offensive or 35% defensive in nature. These percentages are based on how often and critically each skill set is applied in daily tasks, as derived from the job task analysis data (Publication IV, Tables 10–14). For example, the higher proportion of Defensive Skills (35%) reflects the sustained need for securing and hardening systems

before, during, and after OCOs—often forming the baseline from which offensive operations can be considered. The 25% attributed to Offensive Skills doesn't imply planners are spending a quarter of their time gaining unauthorised access to target systems; instead, planning for effects in offensive COs requires substantial domain-specific technical and strategic input. Leadership and Communication are interlaced throughout defensive and offensive activities, supporting coordination, decision-making, and cross-functional teamwork. Figure 6 is best interpreted as a guide to competency emphasis in role-specific training, not as a breakdown of personality or background traits.

Experience

The proposed framework recognises that substantial practical expertise in CO planning roles is essential for OCO planners. These include the ability to conduct offensive and defensive cyberspace operations and to integrate cyberspace considerations into broader military operational planning. Years of military education, practical field experience, and ongoing training contribute significantly to developing this skill set.

The study identifies critical competencies required for OCO planners, encompassing operational, digital, and soft skills. Key digital competencies include cyber situational awareness, network analysis, information security, and risk management. Operational-level skills include doctrinal understanding, targeting, coordination across domains, and cyber weapon employment. Soft skills such as collaboration, adaptability, and decision-making are also central to the planner's role.

Drawing on the NICCS framework [109], Publication IV classifies and aligns these competencies with recognised roles and tasks, such as targeting and cyber mission planning. Training pathways proposed in the framework include cyber warfare courses, network attack simulations, troubleshooting exercises, and applied operational planning within NATO CO exercises or Cyber Headquarters environments.

The article synthesises insights from academic literature, doctrine, and governmental sources to present a role-based framework for the development and evaluation of OCO planners. This framework supports the preparation of planners to function effectively in operational-level cyber commands or multinational exercises.

4.2 Validation of the Proposed Training Framework for OCO Planners

This section addresses RQ1.3: *What framework, including a training plan, skillset, and required competencies, is necessary to develop a competent OCO planner?* Building upon the competency framework introduced in Publication III, Publication IV focuses on validating this training framework through qualitative research involving expert practitioners from NATO countries. The validation aims to ensure that the framework not only reflects theoretical understandings but is also practical and relevant to real-world OCO planning.

A qualitative case study methodology was employed, incorporating semi-structured interviews with experienced OCO planners, using Braun and Clarke's six-step thematic analysis approach [139]. Key themes were extracted relating to the skills, challenges, and operational environment faced by planners in COs. These insights provided essential grounding for assessing whether the proposed training framework effectively captures the evolving demands of cyber warfare and planning.

The validation highlighted several critical dimensions, including the unique temporal dynamics of COs, the importance of strategic and operational planning, and the necessity of technological expertise. Moreover, the experts underscored challenges such as long

preparation lead times, evolving cyber tools, legal and ethical constraints, and the need for trust and interoperability between allied forces.

Notably, the validation process integrated theoretical perspectives with practitioners' real-world experience, reinforcing the framework's applicability and credibility. The interview findings aligned well with existing scholarship and operational norms, emphasising the value of cooperative training programs, mutual trust, and structured, continuous education for OCO planners. The use of rigorous qualitative research standards—such as those outlined by Tracy [103] and Flick [140]—further ensured the study's credibility and resonance.

Overall, Publication IV confirms that the proposed training framework provides a comprehensive and realistic foundation for developing OCO planners' skills in NATO and allied contexts. Its successful validation through expert interviews and case studies demonstrates its suitability for guiding training initiatives in exercises like Crossed Swords and other multinational cyber exercises.

4.3 Optimal Structure for Cyberspace Operations Planning Staff

To provide efficient operational planning and coordination, CO planning professionals must have a thorough understanding of the optimal organisational structure. To address this issue, Publication II examines how CO planning teams can be set up and structured to meet the specific requirements of COs at the operational level.

The study incorporates analysis of current CO planning models, expert interviews, and ideas from NATO doctrines. To ensure smooth integration into joint and combined military operations, it emphasises the need for a multidisciplinary team that strikes a balance between technical expertise and operational leadership capabilities.

Key findings emphasise the significance of properly defined roles and tasks within the planning team. These include specialised roles for operational planners, intelligence analysts, technical cyber specialists, and liaison officers who help coordinate with other domains, including air, sea, and ground troops. The organisational structure must facilitate flexible decision-making while maintaining strong lines of communication to handle the dynamic, fast-paced nature of cyberspace activities.

Publication II also emphasises the importance of integrating cyber planners into larger joint planning cells to improve cooperative planning efforts and promote cross-domain situational awareness. To ensure operational coherence and align cyber consequences with overall mission objectives, this integration is crucial.

According to the study's findings, CO planning staff should have an organisational structure that is flexible, scalable, and responsive to the changing mission needs and cyber threat scenario. Interoperability and efficacy in multinational CO planning initiatives should be further improved by establishing uniform frameworks for responsibilities and team compositions throughout NATO allies.

This section presents the findings addressing Research Question 3 (RQ3): What is the optimal organisational structure for the CO planning staff? The research explores the composition, roles, and coordination mechanisms necessary for effective CO planning, drawing on data from expert interviews, operational observations, and analysis documented in Publication II.

4.3.1 What Is the Optimal Organisational Structure for Red Teams?

Having identified the overarching organisational needs for COs planning, the following subsection turns to the specific structural design of Red Teams. Drawing on empirical data from exercises and interviews, it explores how specialised adversary simulation teams are best structured for effective planning and execution within CO environments.

Publication II uses interviews, previous exercise experiences, and research on COs to develop the ideal organisational structure for Red Teams. Interviews with the Red Team leader from exercise LS [8] 2022, emphasised the value of cohesive sub-teams and adaptability. Twelve years of experience with cyber exercises led to the framework's evolution, emphasising mission planning and execution without the need for elaborate instructions. It should be clarified that while the LS Red Team role-plays elements of adversary strategic and operational objectives, their focus is entirely tactical. This distinction is essential to consider in the context of this thesis, as it highlights the difference between strategic and tactical planning in COs.

The use of sub-teams for network (NET), client-side (CS), and web application (WEB) attacks—derived from practical application with a focus on task specialisation and operational efficiency—led to the proposal of the optimal structure based on insights from Publication III, as illustrated in Figure 7. This structure strikes a balance between functional segmentation and coordination, ensuring effective execution within the constraints of the LS exercise. However, this Red Team structure optimises for LS 2022 and may not apply universally to all OCO scenarios. The research identifies the most optimal range of organisational elements, but further studies must analyse each team's skill set in more depth. This limited sample does not allow researchers to draw a definitive conclusion on optimal team size, and additional studies—potentially examining alternative organisational models, such as those used by cybercriminal gangs—could provide valuable insights for broader applications.

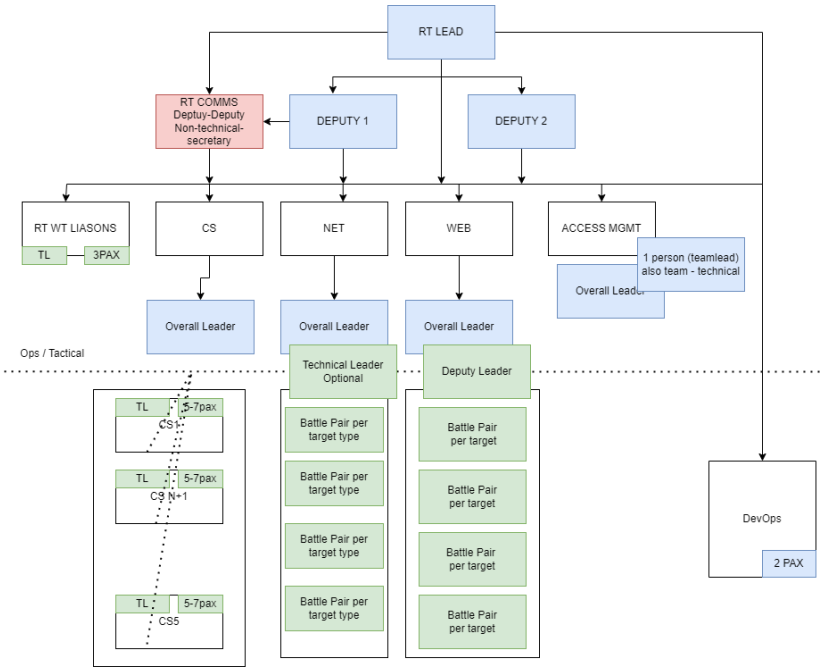

Figure 7. The Optimal Organisational Structure for Locked Shields Red Teams.

The NET team handled network attacks, the Client-Side team planned and carried out client-side attacks, and the WEB team handled web application attacks. The main COMMS and DevOps teams were overseen by the Red Team leader and their two deputies. These handled people and information resources and developed technical tools for the Red Team. In contrast to NET and WEB teams, which were divided into Battle Pairs according to target type, the CS team comprised five sub-teams under the direction of a team leader, each consisting of five to seven subordinates.

4.3.2 What Is the Optimal Organisational Structure for Blue Teams?

The optimal structure for Blue Teams, shown in Figure 8, was derived from empirical team performance analysis during LS 2022 and interviews with team members and exercise planners. The publication reviewed organisational structures from the Blue Teams. The organisational structure components of the leading three Blue Teams varied from 11 to 14, encompassing 8 to 15 components. The study found no clear correlation, suggesting further research is needed. The organisational structure is specific to the current exercise setup and may not be applicable in other contexts.

Subsequent interviews indicated that effective teams started their preparations three to four months ahead, concentrating on technical readiness, strategic planning, and teamwork. In addition, previous studies like the US Marine Corps Cyberspace Training and Readiness Manual [141] and recommendations from CO experts affected the analysis of optimal Blue Team setups. Finally, the literature review in Publication II emphasised early preparation and flexible approaches, endorsing the inclusion of specialist components such as technical capabilities and forensics.

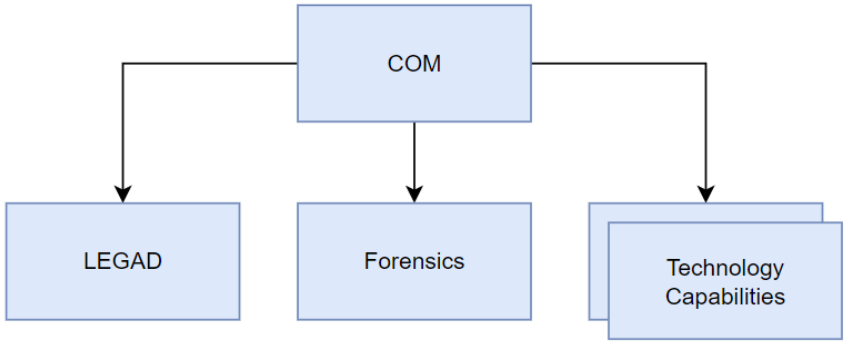

Figure 8. The Optimal Organisational Structure for Locked Shields Blue Teams.

The presence of a commander, legal adviser, forensics, and technological capabilities is essential. Depending on the technical difficulties of the exercise, up to eight distinct technology capability components may be incorporated. Figure 8 illustrates these capabilities: industrial control system (ICS), network, Windows, Linux, monitoring, web, mobile, and threat-hunting capabilities.

4.3.3 Optimal Organisational Structure for Cyber Command HQ

The authors of Publication II propose an organisational structure for the Cyber Command element headquarters (CHQ), which is depicted in Figure 9, based on case studies, interviews, and military theories. Several support functions such as finance, education & training, and logistics—omitted to comply with exercise criteria. This CHQ is an operational-level headquarters exclusively for exercise purposes. This flexible architecture can be used

for various exercises, depending on the training objectives and scenario goals, even if it is not a NATO-standard headquarters structure. To say that this is the universally optimal structure might be a bit much to ask. This organisational structure can be applied to other exercises, depending on the exercise scenario goals and training objectives.

Multiple interviews were conducted with Cyber Headquarters' COS (Chief of Staff) and other planning officers. During those interviews, they shared their thoughts on the importance of C2 (Cyber Headquarters branch for situational awareness), C3 (Cyber Headquarters branch for operations), COS, and Legad (Legal Advisor), among other roles. These positions were shown to be essential for preserving a rational and practical command structure.

To improve the MDMP used in exercises, literature such as the Intelligence Preparation of the Cyber Environment framework from Lemay et al., was consulted [142]. Drawing from literature and real-world operational feedback from exercises such as LS and CS 2022, the study highlights the significance of matching specialists with conventional military forces.

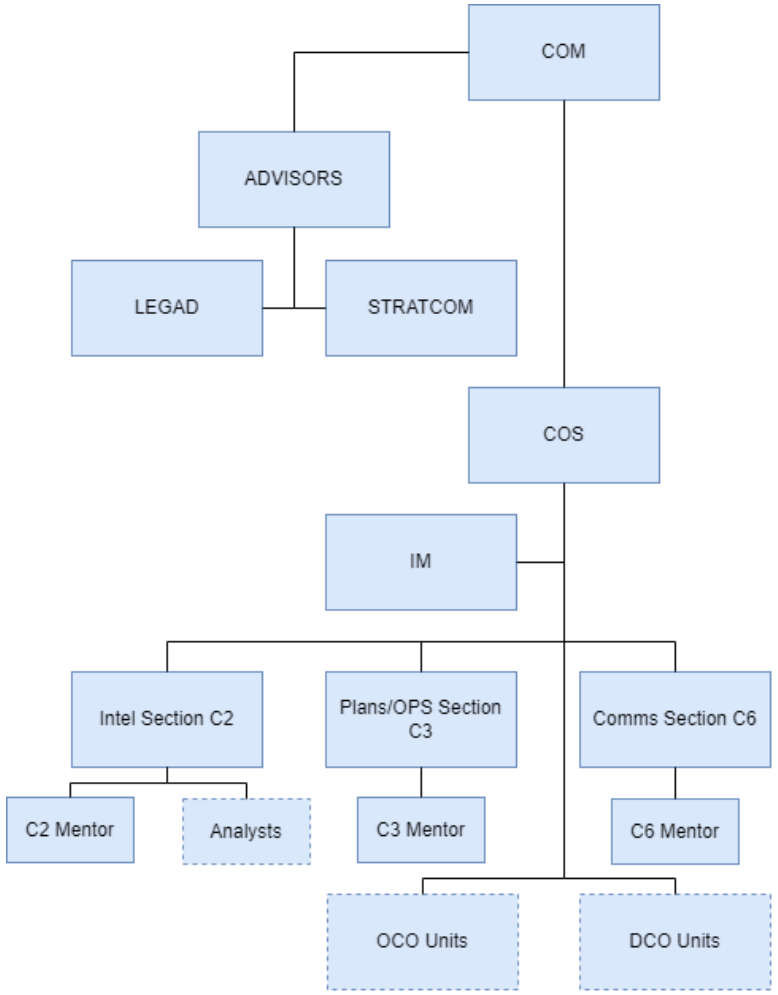

Figure 9. The Optimal Organisational Structure for CHQ.

The Cyber Commander leads and coordinates DCO and OCO to ensure freedom of action in cyberspace and project power. Their tasks include decision support, operational intent, intelligence gathering, joint targeting, rules of engagement, authorisation, situational awareness, and performance assessment. They ensure all actions align with political guidance and military directives, seeking coordination with intelligence partners and other relevant entities throughout the operational planning and execution cycle [41].

Legad role involves maintaining and ensuring systems are operational, conducting necessary CIS Infrastructure Operations, maintaining system status, planning mitigation and business continuity, and ensuring information assurance. It also supports Cyber Defence SMEs in coordinating CIS issues, liaises with NCIA, and advises on national and international laws, regulations, and cyber-related cyber incidents and operations policies. It also proposes offensive cyber aspects, evaluates contracts, and evaluates the effectiveness and efficiency of rules and regulations (Ibid).

Stratcom's goal is to ensure the effective utilisation of strategic communications activities and capabilities in support of Alliance policies, operations, and cyber domain-related activities (Ibid).

COS – chief of staff manages the staff personnel and is second in command.

C2 – situational awareness cell. The primary responsibilities of the situational awareness cell are maintaining situational awareness and cybersecurity in troops, including creating and updating the Recognised Operational Picture, conducting a vulnerability assessment, assessing potential threat actors, and gathering intelligence for cyberspace operations (Ibid).

C3 – operations planning cell. The primary responsibilities of the operations cell are creating and updating the Cyber Prioritised Asset List (CPAL), identifying targets and Cyber Key Terrain (CKT), naming cyber targets, maintaining awareness of cyber dependencies, conducting risk assessments, coordinating mitigation efforts, coordinating cyber intelligence and targeting, de-conflicting cyber battle damage, and monitoring FC/CCs cyber activities (Ibid).

C6 – The communications cell's primary duties include maintaining system functionality, conducting CIS Infrastructure Operations, monitoring system status, planning mitigation, ensuring information assurance, and supporting Cyber Defence SMEs (Ibid).

IM – The information manager is responsible for handling incoming and outgoing data, ensuring correct and timely communication, protecting data security and integrity, prioritising information flow, and assisting in decision-making by gathering and disseminating pertinent intelligence.

The tactical units, separated into OCO and DCO teams, were entirely under the commander's control. In Figure 9, dotted lines indicate live exercise units, whilst solid lines represent the CHQ planning elements. The difficulty in establishing a command structure for a cyber exercise is assigning personnel with the necessary training and experience to critical roles. These comprise technical operators, intelligence, and operations staff to guarantee a transparent and understandable structure for military entities. The precise number of C2 and C3 positions corresponds with the exercise's difficulty level. From the standpoint of CHQ planning, C2, C3, COS[2], and Legad are the most critical positions.

[2] In the given exercise setup, the COS fulfilled the duties of COS and COM.

The study used interviews and questionnaire responses from key personnel, including a COS, a Red Team Leader, a NATO Plans Staff Officer, and a former military officer. The findings are based on expert opinions and case studies, potentially introducing biases.

The research suggests three frameworks for structuring cyber teams: Cyber Command Headquarters (CHQ), Red Teams (Red Teams), and Blue Teams. The CHQ should have a flexible, goal-oriented structure with clear C2 elements. Red Teams should have a leader, sub-teams for different attack vectors, and harmonised teams. Blue Teams should have 11-14 elements and 54-102 personnel, with a commander, legal advisor, forensics, and technical capabilities. Early collaboration and customised software tools are crucial.

The study requires stronger statistical validation and more precise data collection methods to confirm its findings. While it provides a solid conceptual framework, further research is needed to generalise findings beyond military exercises.

4.4 Planning Challenges in the Logical Layer

The logical layer in CO—representing network relationships, system vulnerabilities, data flows, and cyber defences—is critical yet challenging for operational planning and situational awareness (SA). To mitigate these challenges, leveraging simulation tools and operational visualisation frameworks is essential.

Visualisation and Simulation examples of tools for improving logical layer understanding are:

- CyCOP: A command-and-control system that integrates physical and cyber data sources like NATO Vector Graphics (NVG) and OSSIM for real-time Cyber Hybrid Situational Awareness (CyHSA). It offers 2D/3D charts, dynamic diagrams, and geo-located representations, facilitating a comprehensive view of the cyber domain [143], [144].
- VISA (Visualisation for Improved Situation Awareness): This tool uses advanced visualisation principles to provide a high-level operational picture, focusing on cyber threats and assets. It adapts military symbols to represent cyber elements better, including individual CIS components and network structures, enhancing situational awareness [143], [93].
- MIL-STD-2525D: While primarily designed for conventional military domains, this military symbology framework can be adapted to represent cyberspace objects using graphical symbols, helping to visualise cyberspace-related elements and activities in a standardised format [145].

These tools aim to simulate and visualise operational elements, capabilities, and effects across the physical, logical, and cyber-persona domains—addressing the inherently multi-domain nature of contemporary military operations. The growing demand for simulation tools that effectively represent all operational domains is well documented [146]. While training simulations are often associated with Modelling and Simulation (M&S), other valuable applications include operational analysis and COA development.

As noted in the NATO Modelling and Simulation Capability Programme study, federating multiple simulations across operational domains via High-Level Architecture (HLA) can be advantageous for training. However, direct integration may not always be feasible due to disparities in time scales and unit levels. In such cases, using complementary models in a coordinated and systematic manner remains a viable solution [147].

CO planning relies on understanding three critical layers:

- Physical Network Layer: Tangible infrastructure, including hardware, command systems, and communications nodes, is essential for identifying cyber terrain and potential adversary entry points.
- Logical Network Layer: Interconnections, vulnerabilities, access controls, and data flows are vital for anticipating adversary actions and designing defensive measures.
- Cyber-Persona Layer: The human element, encompassing cyberspace actors and their behaviours, is crucial for planning influence operations, deception, and intelligence activities.

Operational visualisation tools enhance cyber situational awareness by mapping and linking assets, highlighting logical relationships and potential threats, applying standardised or adapted symbology, incorporating real-time data streams, automating scenario simulations, and leveraging 3D or mixed reality environments for complex scenarios. These capabilities improve team communication, shared situational awareness, and rapid decision-making.

Operational visualisation tools enhance cyber situational awareness by mapping and linking assets, highlighting logical relationships and potential threats, applying non-technical symbols, incorporating real-time data streams, automating scenario simulations, and utilising 3D and mixed reality visualisations for complex scenarios, thereby improving team communication and shared situational awareness, especially in rapid-response situations.

Survey data indicates that over 70% of participating experts prioritised the need for tailored tools for CO planning. Key user requirements include:

a) Clear visualisation of assets and connections.
b) Dynamic, real-time data integration.
c) Standardised or adaptable symbology.
d) Automation features.
e) Compliance with existing operational frameworks.
f) Support for advanced visualisation modes (e.g., 3D, mixed reality).

These findings underline the necessity for tools that reflect the operational realities of cyberspace operations, ensuring efficient coordination, improved decision support, and reduced cognitive workload.

This section addresses RQ3: *How can operational planning and situational awareness for cyberspace operations be enhanced?* The analysis integrates empirical data, expert insights, and existing literature to identify core challenges and propose actionable solutions, as detailed in Publication V.

In conclusion, integrated simulation and visualisation techniques that incorporate network relationships, physical infrastructure, and human aspects are essential to address logical layer challenges in cyberspace operations effectively. By adopting operational visualisation tools like CyCOP and VISA and applying flexible frameworks such as the three-layer model, cyber planners can improve situational awareness, inform decision-making, and enhance mission outcomes. The emphasis on accessibility, automation, standardisation, and multi-dimensional visualisation in future CO Planning Tools is firmly validated by user-driven requirements. As introduced in Chapter 2, the three-layer model frames the cyberspace domain. This section applies that model to challenges encountered in operational planning.

4.4.1 Essential Layers in Cyberspace Operations Planning

Publication V examines the fundamental levels of CO planning and shows how they support the successful execution of cyber missions. In the context of CO planning, several frameworks have been reviewed to evaluate their effectiveness in supporting mission execution. These frameworks are designed to guide the planning, execution, and assessment of COs across military and organisational domains. Below are the key frameworks considered.

NATO's Allied Joint Doctrine for Cyberspace Operations [25]. This framework guides joint operations planning, integrating voluntary cyber effects from allies into alliance missions. It highlights the importance of interoperability and adaptability in multi-national settings.

LandCyber Framework [148], this framework, developed as part of the US Army's strategy for COs from 2018 to 2030, emphasises a unified approach to COs, facilitating enhanced coordination and operational understanding.

Trilateral Strategic Initiative, this framework, focused on improving operational assessment, interoperability, and trust in COs, is an emerging model for enhancing agility and adaptability within the cyber domain [149].

Cyber-FIT Version 4, this simulation framework addresses team performance modelling in contested cyber environments. It supports agile development processes and enables effective planning for COs, ensuring that new technologies, vulnerabilities, and patches are managed optimally [78].

The NIST Cybersecurity Framework focuses on security control assessments and risk management in federal organisations. It enhances understanding and readiness for cyber threats and integrates operational requirements into training processes [80].

CyCOP, a framework that supports enhancing situational awareness (SA) by providing a unified operational picture of cyberspace activities and incidents, enabling better decision-making and planning [93].

Military Symbology Standards (MIL-STD-2525D): This military standard provides a visual language for representing operational elements in cyberspace, which is crucial for conveying operational details, particularly in command-and-control scenarios [145].

The review shows key distinctions between the various COs frameworks: Although they provide broad perspectives, NATO's AJP-3.20 and LandCyber do not specifically address cyber domain layers. Team performance modelling is the main focus of the Cyber-FIT and Simulation Frameworks; however, they do not mesh well with operational-level decision-making. The CyCOP framework emphasises cyber mission visualisation and real-time situational awareness.

The physical, logical, and cyber-persona Network model offers the most effective framework for supporting CO planning by integrating the physical, logical, and human dimensions of the cyberspace domain. This model enhances flexibility, situational awareness, and decision-making, enabling planners to better adapt to dynamic and contested environments. In particular, the logical layer of this model corresponds to the primary cyber terrain—the network—which, much like areas of operation in the physical domain, serves as the operational space within which forces manoeuvre and conduct missions. Governed by policies from Domain Accreditation Authorities and protected through defensive measures such as firewalls and intrusion detection services, networks become fortified operational areas [81]. This alignment with established operational concepts enhances the model's ability to provide critical insights at both tactical and

strategic levels, making it especially well-suited to contemporary CO planning requirements.

The article methodically explains the function of each layer in executing a cyber mission. It describes how planners may develop workable COAs to fend off threats and safeguard assets by thoroughly understanding these layers.

The Three Crucial Levels of Planning for Cyberspace Operations:

1. Physical Network Layer. The operational environment's physical infrastructure is part of the physical layer. It comprises threat Command and Control systems, network devices, access points, and important nodes. For both offensive and defensive cyber activities, this layer is essential. Planners can Identify vital cyberspace terrain, Secure mission-critical assets, and more by mapping and analysing the physical infrastructure. Identify points of entry for enemies. By guaranteeing that the physical foundation of cyberspace stays secure and operable, an understanding of this layer enhances mission resilience.
2. Layer of the Logical Network. The logical layer represents the connections between networks, systems, and data flows. It covers intrusion detection systems, network settings, vulnerabilities, encryption techniques, and access controls. This layer is crucial for mission planning since it where cyberattacks and defences take place. Cyber planners can Predict enemy movements based on system vulnerabilities by analysing logical interactions. Boost situational awareness by monitoring network activity. Create countermeasures that interfere with the activities of the enemy. According to the study, situational awareness in this layer directly impacts mission accomplishment by enabling planners to anticipate, stop, and respond to cyber threats effectively.
3. Layer of Cyber-Persona. The cyber-persona layer focuses on human players in cyberspace, such as users, hackers, cyber warfare units, and other stakeholders. This layer is essential for influence efforts, deception operations, and cyber intelligence. The article highlights that integrating cyber-persona analysis into CO planning improves decision-making by fusing technological insights with behavioural intelligence.

Contributions to the Execution of Cyber Missions. Using this multi-layered strategy, planners can create cyber strategies incorporating human elements, network interactions, and physical infrastructure. They can also find weaknesses in the three layers to improve risk management. They can optimise offensive operations and cyber defences to guarantee that COs are carried out effectively.

The article's results demonstrate that the three-layer model, which offers an organised approach to planning and executing COs, is crucial for mission accomplishment. In COs, situational awareness is derived primarily from analysing the logical network layer. This layer is crucial because it allows planners to assess the advantages, disadvantages, and potential risks of offensive and defensive actions. By mapping the logical network layer, planners can identify key systems, vulnerabilities, and social interactions and track how mission-critical data is accessed or shared. This three-layer model ensures a comprehensive approach that combines technical infrastructure and human factors, optimising CySA and enabling planners to make more informed decisions. This model is derived from real-world COs and aligns with the framework used in exercises such as LS and CS. As mentioned in the IPB guidelines, the logical and physical layers, along with an understanding of baseline activity and infrastructure, are fundamental to effective mission planning and execution [52].

4.4.2 Enhancing Cyber Situational Awareness with Visualisation Tools

After analysing the foundational cyberspace layers and their relevance to planning, this subsection focuses on how situational awareness can be operationally enhanced. Specifically, it explores how visualisation tools and technologies contribute to decision-making effectiveness in COs by making abstract cyber terrain visible, interactive, and actionable.

Publication V discusses several concepts and crucial methods for improving cyber situational awareness in COs using operational visualisation tools. The primary resources and methods are mentioned as follows.

CyCOP provides real-time CyHSA by leveraging both cyber and physical data sources, such as Open Source SIEM (OSSIM) and NATO Vector Graphics (NVG) protocol. CyCOP provides dynamic diagrams, geo-located visualisations, and 2D/3D charts for flexible data representation. It implements Cyberspace Symbol Components from MIL-STD, using hexagons with symbols or characters to clarify cyberspace representation [143].

The Royal Military Academy's 3D Operational Picture uses innovative 3d visualisation software to maximise operator awareness during cyberattacks and improves comprehension of the consequences of cyber protection by offering high-level abstraction with specific perspectives when zoomed in (Ibid).

VISA enhances situational awareness using cyber symbols and representations of tools and services. It uses design concepts complementing current military symbols to improve interpretability. When magnified, VISA uses abstract nodes that break down into specific CIS components, offering high-level and in-depth operational perspectives (Ibid).

Cyber Order of Battle and Risk Assessment integrates mission planning and risk assessments to facilitate an educated and flexible decision-making process. proposes experimental verification to improve military commanders' cyber situational awareness systems (Ibid).

MIL-STD-2525D Symbology uses various expressive techniques, such as frames, icons, and fill for graphic representation, to adapt traditional military symbology to cyberspace. This method helps quick decision-making during COs by enabling precise mapping and cyberspace visualisation [145].

Operational Picture Concepts and Cognitive Dimension Integration enhances decision-making and cross-domain operations by combining cognitive and virtual aspects with operational picture principles. It allows commanders to act at network speed by supporting real-time situational understanding [148].

The effectiveness of the OCO Risk Framework with Graphical Outputs in supporting decision-making is demonstrated, particularly for staff members with little experience. It reduces the requirement for national-level expertise by communicating risk evaluations using graphical representations [150].

Abstract Visualisations for Data Contextualisation highlights how crucial it is to contextualise data rather than visualise all the data that is accessible to ensure clarity and better decision-making. It reduces noise and enhances operational knowledge by summarising massive datasets using abstract representations [151].

These visualisation tools and frameworks improve cyber situational awareness by integrating real-time data integration, standardised military symbology, risk assessment, and sophisticated visualisation techniques. In COs, they facilitate dynamic decision-making and efficient communication of intricate cyber circumstances.

Every tool under review had some features essential for organising and executing COs. None of them, however, completely satisfied the prerequisites for an OCO planning tool.

This disparity emphasises the need for a more thorough approach. The author suggests his prototype in the next chapter to overcome these issues and improve OCO planning capabilities.

Among the key findings are essential CO planning levels. According to the publication that examined many definitions of the cyberspace layers, the logical network layer is the most crucial for structuring COs. Understanding and executing successful COs requires understanding the relationships and interactions across cyber assets, which are the emphasis of this layer. Situational awareness is derived from analysing the logical network layer, enabling planners to assess advantages, disadvantages, and potential risks, helping them design informed defences against cyberattacks. By mapping the logical network layer, planners can identify key systems, social interactions, and vulnerabilities and track how mission-critical data is accessed or shared. Furthermore, reporting from multiple sources enhances the understanding of threat cyberspace, including network protocols, IP addresses (Internet Protocol address), operating systems, and the methods used to intrude and mask activity. Understanding the logical and physical network layers, baseline activity, and key infrastructure is essential for effective defence planning [52].

Publication V proposes a logical-layer visualisation tool called Cyber Planner tool to improve situational awareness, plan and execute cyberspace operations more effectively, evaluate operational environments, and create well-informed strategies for intricate cyber missions.

Operational visualisation tools can increase CySA in various ways. Tools such as the Cyber Planner thoroughly evaluate operational areas, defining key cyberspace terrain and mapping approach routes. These technologies provide dynamic logical connections across cyber assets, enabling in-depth analysis and enhanced decision-making. Successful mission planning and execution depend on military personnel and cybersecurity specialists coordinating and communicating more efficiently, which is made possible by improved visual tools.

Operational visualisation tools enhance cyber situational awareness and facilitate effective CO planning. The article identified thirty user requirements for the CO Planning Tool through an online poll, interviews, literature analysis, and experiences from prior exercises. These approaches, which incorporate feedback from subject-matter specialists and thorough literature reviews, highlight how crucial it is to incorporate user needs and pre-existing frameworks when creating CO visualisation tools (Table 5).

4.4.3 User Requirements for the Cyberspace Operations Planning Tool

The publication V identified thirty user requirements for the CO Planning Tool through an online survey, interviews, literature review, and previous exercise experiences based on subject-matter experts and literature review (Table 5).

The user requirements in Table 5 were identified and consolidated using a mixed-method approach. Including a structured online survey, semi-structured interviews with cyber exercise experts, a comprehensive literature review, and participant observation and after-action reporting from real-world cyber exercises and simulations.

Table 6. Identified User Requirements for the proposed Cyber Planner Tool.

	User Requirement	Source
1	Interface with well-known frameworks such as AJP-3.20, LandCyber, and NIST for compatibility.	Review
2	Provide sophisticated visualisation tools to help commanders comprehend activities in cyberspace.	Interview
3	Facilitate data sharing and communication between systems for improved interoperability.	Review
4	Include simulation and rapid development features to maximise preparation and execution.	Interview
5	Incorporate risk management frameworks and support both offensive and defensive cyberspace operations.	Review
6	Analyse political conflicts based on cyberspace and offer decision assistance.	Interview
7	Provide real-time information management and a comprehensive operational picture.	Interview
8	Enhance visibility through icon design and enable threat behaviour analysis.	Review
9	Offer comprehensive visualisation capabilities and contextualised information representation.	Interview
10	Integrate 3D mixed reality visualisations for improved human-to-human communication.	Review
11	Support tailored training and skill development for cyber operations analysts and planners.	Interview
12	Include predictive analytics for forecasting potential threats.	Review
13	Dynamically present data to aid in detecting and managing cyber threats.	Interview
14	Integrate human factors, making complex data comprehensible in real-time. **(New)**	Interview
15	Design CSA tools with practical features that align with SME resource constraints.	Review
16	Provide multi-layered visualisation of the cyber environment, including systems, personas, and connections.	Interview
17	Include filters to find connections between different entities quickly.	Review
18	Use colourful and simple symbols, avoiding obscure acronyms.	Interview
19	Display detailed asset properties on mouse-over.	Review
20	Allow for the combination of assets and connection to physical infrastructure layers.	Interview
21	Integrate APIs for mapping Tactics, Techniques, and Procedures (TTPs) to frameworks like MITRE. **(New)**	Review
22	Group networks are used to easily view and implement a target approval status system.	Interview
23	Integrate asset information with situational awareness for comprehensive management.	Review
24	Sync asset visual modifications with backend databases and simulate significant events for better understanding. **(New)**	Interview
25	Enable advanced information management and data exchange functionalities.	Review
26	Provide a (strategic) overview of forces, IT systems, and risks, aligning with joint functions.	Interview
27	Enable real-time battle damage and operational assessments for strategic decision-making.	Review
28	Automate the planning process and integrate real-time data for dynamic scenario simulations.	Interview
29	Standardize symbols for clarity and consistency across operational levels.	Review
30	Ensure compatibility with NATO planning systems (and include strong filtering capabilities). **(New)**	Interview

The 2020 and 2022 Crossed Swords exercises significantly improved the Cyber Planner tool that was introduced in Section 3.2. This enhanced operational planning and situational awareness in COs and highlighting the need for better tools for operational visualisation. These experiences influenced many standards for improving operational planning and situational awareness in COs. This further illustrated the need for better tools for operational visualisation. The goal of the study was to address real needs in COs. The following are necessary conditions for the CO Planning Tool. These requirements are based on the insights gained from the interviews and surveys. The study aimed to address real needs in COs by capturing user requirements directly from the target audience.

Visualising Operational Areas and Assets: To facilitate situational awareness and decision-making, the tool must provide a clear and organised visual representation of Blue, Red, and third-party assets and logical links between them.

Dynamic and Logical Connections: The tool should allow for dynamic linking between assets to enhance the planner's ability to map out relationships, approaches, and essential terrain inside the cyberspace domain.

Enhanced Symbolism: Simple, colourful symbols that avoid cryptic jargon are necessary to appeal to people with backgrounds in ICT and cybersecurity. Standardised symbols would strengthen communication and usability.

Incorporating filters and amplifiers can enhance targeting, persona analysis, and network evaluation while assisting planners in concentrating on specific areas of interest.

Automation: The tool must integrate real-time data, automate portions of the planning process, and enable dynamic scenario simulations to boost productivity and decrease repetitive tasks.

Integration with Standards: For improved data sharing, risk management, and planning procedures, the tool should be integrated with current frameworks such as AJP-3.20 [25], MITRE [42], and others.

Visualisations in 3D and Mixed Reality: The tool should facilitate visualisations in 3D and mixed reality to enhance human-to-human communication. This feature was confirmed to apply based on survey replies. The tool should enable 3D and mixed-reality visualisations to improve human-to-human communication. 2D visualisations are adequate for static network diagrams and incident timelines. However, 3D and mixed reality are necessary for complex COs and rapid response coordination. Mixed reality enhances situational awareness and decision-making by allowing real-time interaction between team members, especially during high-stakes exercises or operations requiring rapid cyber threat adjustments.

More than 70% of respondents to a COs experts survey said these characteristics were essential for improving situational awareness and operational planning, which strongly supported these criteria.

In addition to the publication, most recent studies support existing user requirements, such as visualisation tools, interoperability, predictive analytics, training environments, and NATO system compatibility [146]. Later research also identified new user requirements, such as balanced fidelity, explicit command, control, and communication modelling, cross-domain sensor-effect integration, after-action review/playback, and AI-based behaviour modelling (Ibid). Combining these with the author's identified user requirements will result in a suitable planning tool for planners for future COs.

The study confirmed most user needs using expert interviews and a literature review, which increased confidence in their applicability to CO planning. However, only interviews were used to validate some requirements, which may have introduced prejudice or

constrained viewpoints. New and unvalidated requirements were found to have low confidence, indicating that they should be given priority for future validation as they lack empirical support (Table 5). Although the mix of expert interviews and literature reviews provides a strong methodological approach, inconsistencies suggest additional research. Overall, confidence is low for new and unvalidated requirements that need more testing or stakeholder input. However, it is moderate to high for validated requirements backed by literature and interviews.

4.5 The Proposed Cyber Planner Tool

The Cyber Planner Tool, developed and deployed during the CS 2021 exercise, serves as an essential domain-specific solution to address the complex challenges of CO planning (Figure 10). Based on user feedback and expert insights documented in Publication V, the tool's iterative development has validated its core functionalities. While there remain gaps in specific user requirements, the Cyber Planner Tool proves to be an effective support system for planners. The tool addresses key challenges in cyber situational awareness, coordination, and real-time decision-making by integrating findings from previous research, such as the identified competencies and operational layers crucial for CO planning.

Publications I and II emphasised the importance of incorporating multi-layered cyber intelligence across physical, logical, and cyber-persona layers for effective CO planning. These layers must be considered holistically to enhance decision-making and ensure operational success.

The Cyber Planner Tool integrates these layers, enabling planners to model and simulate complex COs scenarios. It uses standard ICT symbols, such as routers, servers, and network nodes, which are intuitive for cyberspace planners with ICT backgrounds. This symbol usage facilitates a clear visual representation of cyber infrastructures, improving situational awareness and enabling real-time operational adjustments. The tool allows planners to map out and visualise critical assets, such as industrial control systems in OCOs (e.g., CS), by tagging metadata to identify vulnerabilities and threats at each layer. The tool's ability to map cyberspace activities ensures informed decisions, aligning with research findings that multi-layered intelligence is crucial for successful CO planning.

As highlighted in Publications III and IV, a mix of technical, operational, and decision-making skills was crucial in examining the competencies required for successful CO planning. These include the capacity to evaluate risk, comprehend the consequences of cyberattacks, and plan activities across several domains.

By enabling scenario-based simulations and real-time decision-making, the Cyber Planner Tool promotes competency development. Planners can manage risks, rehearse offensive and defensive goals, and model different cyberattack scenarios. Both technical (such as identifying vulnerabilities and breach points) and operational (such as coordinating multi-domain responses to cyber incidents) competencies are developed using this practical method. The tool's user-friendly interface also encourages cooperation between planners with different specialities, including academic, military, and civilian players, improving their combined capacity to carry out intricate cyber tasks. The tool helps to build and strengthen the skills identified in the research by providing a platform for active learning and practice with real-world situations, strengthening CO planners' operational readiness.

Publication V identified new Cyber Planners Tools user requirements and highlighted the need for enhanced cyber situational awareness to address COs rapid and complex nature. This includes the integration of intelligence, the ability to track adversary tactics,

techniques, and procedures (TTPS), and the need for up-to-date visualisations that reflect the dynamic nature of the cyber domain.

The Cyber Planner Tool meets this need by offering advanced visualisation capabilities representing network topology and adversary activity. Through features such as TTP mapping, MITRE ATT&CK integration, and metadata tracking, the tool enables planners to visualise and track critical assets' status in real time, helping them stay ahead of adversaries. The ability to simulate various cyberattacks and defence scenarios ensures that planners can make well-informed decisions backed by real-time data. The tool's real-time visualisations and intelligence integration directly support the findings from Publications II and V, emphasising the need for situational awareness as a critical enabler of effective CO planning.

Publication II underscores the complexity of conducting EBO in the cyber domain. Understanding how cyber effects impact military operations and vice versa is essential for effective mission planning.

The Cyber Planner Tool enables planners to simulate and visualise effects-based operations, clearly representing how COs can influence broader military objectives. It facilitates the identification of target systems, the mapping of logical and physical infrastructure, and the tagging of critical assets. The tool's ability to provide metadata on enemy and friendly forces allows planners to quickly identify vulnerabilities and develop a coordinated, multi-faceted response in COs. The Cyber Planner Tool directly supports EBO by integrating cyber effects with broader military objectives, which aligns with the research findings from Publication II about the need for effective EBO in cyber missions.

This research identified the critical need for coordination across multiple shifts and real-time data integration to enhance continuity during long-duration missions. The Cyber Planner Tool addresses this by providing persistent operational views and comprehensive metadata reporting. This functionality ensures that new shifts can quickly understand the status of assets, ongoing operations, and prior actions.

The tool's reporting capabilities include the status of critical assets, such as whether adversary systems are compromised or if the owner's systems are secure. This data-driven approach allows for evidence-based decisions on whether to escalate operations or reinforce defences, ensuring a smoother transition between shifts and greater continuity of planning. The Cyber Planner Tool supports long-duration mission planning by providing continuity of situational awareness and data-driven decision-making, as emphasised in the findings of Publications I and II.

Integrating research findings on multi-layered cyber intelligence, required competencies, cyber situational awareness, and the challenges of EBO directly informs the design and functionality of the Cyber Planner Tool. The tool addresses gaps identified in the research, such as real-time data integration, TTP mapping, and simulation support, offering a solution that enhances the effectiveness of COs planning. This fusion of theoretical insights with practical tool development highlights how the Cyber Planner Tool can bridge the gap between traditional operational planning approaches and the unique demands of the cyber domain, offering planners an intuitive, data-driven platform to conduct real-time, multi-layered COs. The next development milestone is the tool's evolution toward technology readiness level TLR 5 [152]. Thorough validation procedures, improved risk management, strong logical and physical layer modelling, and the integration of enemy and allied asset data are all necessary. Verification through involvement in multinational CO exercises will be essential to ensure the technology is dependable, operationally appropriate, and improves the cyber readiness of allied forces.

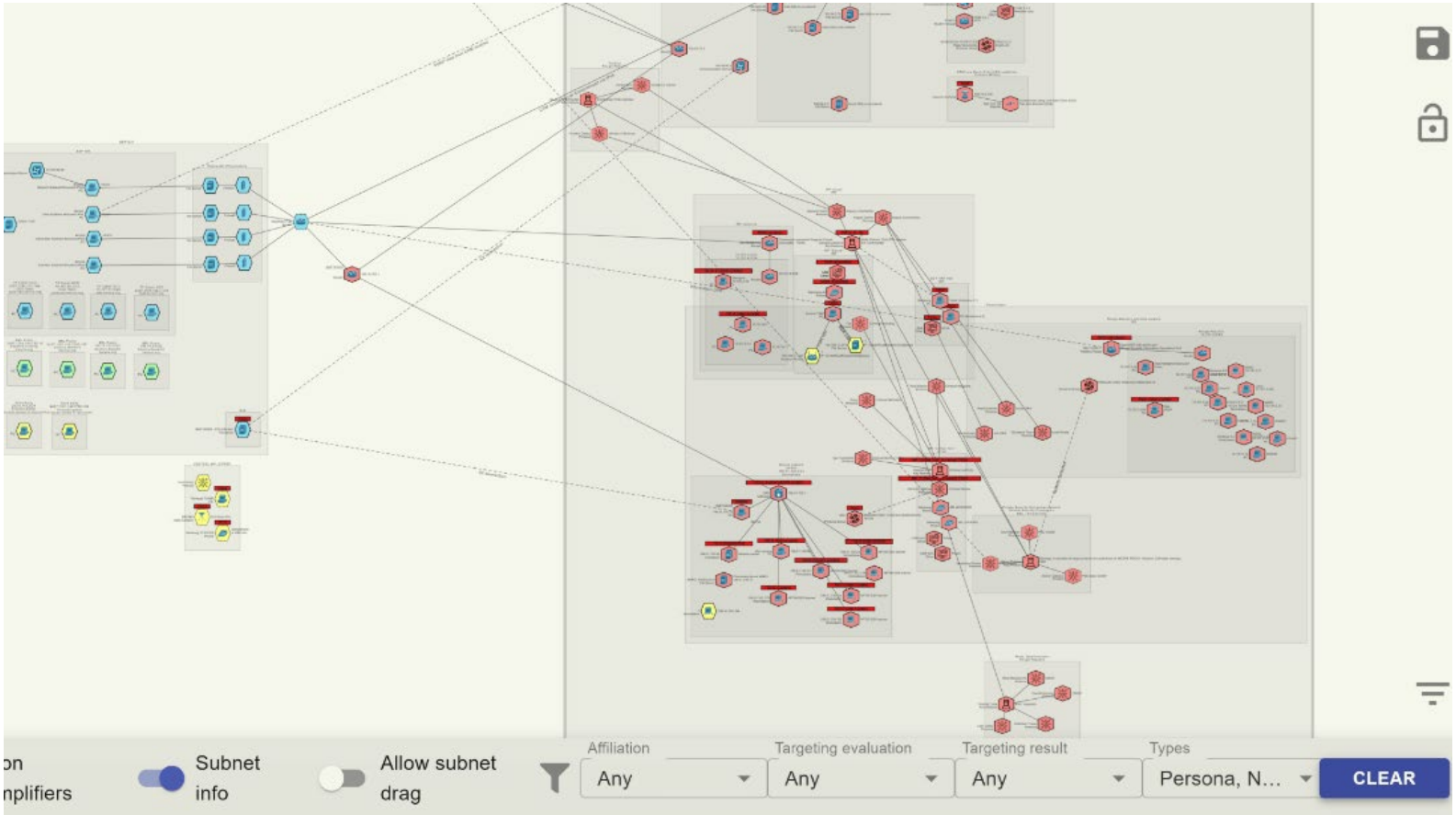

Figure 10. Overview Of Proposed Cyber Planner Tool.

4.6 Consolidated Synthesis of Research Results

Sections 4.1–4.5 provided detailed, individual analyses of the empirical findings from interviews, exercises, prototype testing, and operational artefact studies. This section now consolidates these findings in alignment with the three overarching Research Questions and integrates evidence from Publications I–VI. The following synthesis presents the core results and contributions of the thesis to the field of cyberspace operations planning and situational awareness.

This section consolidates the findings of this thesis by presenting them according to the three Research Questions (RQs) introduced in Chapter 1.2 and discussed throughout Chapters 4.1–4.5. It integrates evidence from the author's six peer-reviewed publications (Publications I–VI), illustrating how these studies collectively reinforce and extend the research outcomes presented in this thesis. The results are structured around each RQ, drawing from new findings and prior publications to provide a unified, evidence-based understanding of operational planning and situational awareness for CO.

4.6.1 Answering RQ1: Competencies Required for Offensive Cyber Planners

This was significantly expanded in Publication III, which systematically identified and categorised required competencies for offensive CO planners through operational interviews and literature synthesis. It established that competencies fall into four clusters: operational planning, technical execution, cyber threat intelligence, and legal and ethical compliance—each vital for mission assurance in dynamic and contested cyber environments.

Sections 4.1 and 4.2 of this thesis reinforced these conclusions, particularly the importance of understanding adversary TTPs, cross-domain coordination, risk assessment, and synchronised decision-making. Publication I called for increased use of exercises and simulations, aligning with the proposed tailored training framework detailed in Publication IV, which further examined how offensive CO planners' competencies can be progressively developed through structured, exercise-driven pathways and a competency-based training model.

Together, these results demonstrate that CO planners require a multi-disciplinary skill set, validated through operational testing, exercises, and specialist training pathways—a conclusion substantiated by Publications I, III, and IV.

4.6.2 Answering RQ2: Optimal Organisational Structure for CO

This research question addressed the organisational models necessary for the effective planning and execution of CO within military frameworks. Publication I established that cyberspace requires distinct structures, proposing that a dedicated Cyber Headquarters (CHQ) or a specialised cyber staff element within Joint or Component Commands is essential due to the domain's technical complexity and operational demands.

Publication II built upon this, offering a structured analysis of optimal organisational models based on operational observations from major NATO exercises. It identified key characteristics for effective CO structures:

- Specialised cyber effects cells for planning and coordination.
- Integrated intelligence and situational awareness functions.
- Clear command and control arrangements to manage national caveats, operational security, and legal oversight.

Further operational validation came from Publication III, which examined competency profiles and organisational roles in CO teams. It recommended integrating functions such as cyber threat intelligence, effects coordination, operational planning, and legal advisory, while ensuring redundancy, cross-training, and operational continuity.

These findings, validated by practical insights from exercises like Crossed Swords (CS) and Locked Shields (LS), confirmed that the absence of harmonised planning processes, unified staff competencies, and integrated intelligence cells undermined operational success.

An optimised CO organisational model should therefore:

a) Be dedicated and autonomous within Joint/Component Commands.
b) Maintain role-differentiated structures comprising planners, technical SMEs, effects coordinators, and legal/intelligence officers.
c) Integrate intelligence functions for continuous threat monitoring and operational decision support.
d) Align with NATO command structures for seamless coordination with conventional forces and allied CO capabilities.

This model addresses command, control, and integration challenges identified in prior research and operational exercises, providing a validated organisational framework for NATO and national armed forces' CO operations.

4.6.3 Answering RQ3:Enhancing Planning and Situational Awareness in COs

The third research question examined how operational planning and situational awareness can be improved in CO contexts. Publication V systematically identified and verified user requirements for a CO planning tool through workshops, interviews, and operational testing.

4.6.3.1 Identifying User Requirements for the Cyber Operations Planning Tool

Through an iterative process involving operational experts and CO practitioners, Publication V identified the following key user requirements:

a) Persistent, multi-layered operational visualisation of mission impacts, ongoing operations, and adversary activity.

b) COA modelling capabilities that account for mission goals, dependencies, and potential adversary reactions.

c) Access to up-to-date adversary TTP (Tactics, Techniques, and Procedures) libraries for threat-informed situational awareness.

d) Real-time information and event correlation to support rapid decision-making.

e) Standardised, NATO-compatible planning workflows to ensure interoperability and procedural coherence.

f) API-based interoperability with C2 systems, cyber ranges, and threat intelligence platforms to enable data-driven planning.

These requirements collectively addressed critical gaps identified in earlier works (Publications I and II), which had emphasised the need for improved operational visualisation, technical-operational synchronisation, and intelligence integration across planning processes.

4.6.3.2 Validation through Prototyping and Operational Testing

The development and operational testing of the Cyber Planner Tool prototype (as detailed in Section 4.5) confirmed that the inclusion of the above capabilities significantly enhanced planners' situational awareness and operational coherence in contested cyber environments.

Publication V consolidated insights from prior research into a comprehensive, operationally validated set of user requirements. This validation demonstrated that when planners are supported by tools integrating real-time data, adversary modelling, and interoperable workflows, their ability to visualise, anticipate, and coordinate CO improves markedly.

4.6.3.3 Situational Awareness and Decision-Making Enhancement in CO

Situational awareness in CO remains inherently complex due to its multi-layered, dynamic nature. Publication V underscored the critical need for synchronised, multi-source intelligence to support operational decisions. This was reinforced by Publication I, which argued that EBO in cyberspace requires multidimensional dependency awareness and anticipation of unintended consequences. Sections 4.3 and 4.4 identified gaps in intelligence integration and operational visualisation, highlighting them as key inhibitors to mission success.

In response, Section 4.5's Cyber Planner Tool addressed these challenges by implementing:

a) Multi-layered operational visualisation.
b) Real-time adversary TTP libraries.
c) Persistent event correlation and metadata-driven reporting.
d) NATO-compatible planning workflows.
e) Integrated technical-operational intelligence feeds.

These validated requirements, derived primarily from Publications V and I–IV, form a solid operational foundation for improving decision-making and situational awareness in CO.

The thesis's core findings emphasise the importance of a competency-based, role-differentiated organisational model for CO, enhanced situational awareness tools, risk assessment capabilities, and intelligence integration. It also emphasises the need for formal integration of user requirements into NATO CO planning processes, tool development, and training frameworks. The framework addresses capability gaps and offers actionable recommendations for enhancing military CO planning and execution capabilities.

4.6.4 Summary of Key Findings

This section consolidated and synthesised the main findings of this thesis by systematically addressing the three overarching Research Questions through evidence drawn from the six constituent publications and empirical work conducted during exercises and prototype testing.

The analysis confirmed that effective operational planning and situational awareness for CO require:

1. A clearly defined set of operational, technical, and intelligence competencies for CO planners, distinct from those required in conventional military domains. These competencies must encompass adversary TTP awareness, cross-domain

targeting, technical infrastructure understanding, risk assessment, and operational synchronisation, validated through targeted exercises and training frameworks.

2. A dedicated, role-differentiated organisational structure for CO within military command frameworks, featuring integrated intelligence functions, cyber effects planning cells, operational planners, technical SMEs, and legal advisors. This structure must provide clear command and control, operational security, and seamless coordination with conventional forces and allied capabilities.
3. The operational necessity for enhanced situational awareness tools and planning support systems, capable of providing multi-layered operational visualisation, persistent metadata management, adversary TTP libraries, and NATO-compatible planning workflows. The validated user requirements gathered in this thesis informed the development and operational testing of the Cyber Planner Tool, demonstrating its potential to enhance operational coherence, situational awareness, and decision-making in contested, dynamic cyber environments.

Collectively, these findings address key capability gaps identified in previous research and operational exercises. They contribute a validated, evidence-based framework for enhancing operational planning and situational awareness in COs, aligned with NATO doctrinal principles. This consolidated understanding directly informs future CO training, organisational development, operational planning processes, and technology integration within NATO and allied forces.

5 Discussion

This chapter critically reflects on the findings presented in the constituent articles of this thesis, placing them within the broader academic, operational, and doctrinal context of COs. Given the complex and dynamic nature of COs, enhancing operational planning and situational awareness has become imperative. The discussion is organised around five core thematic areas, each addressing a significant aspect of cyberspace operations as illuminated through the cumulative research contributions of this work.

5.1 Experience-Related Findings

The findings on the practical experience and competencies required for OCO planners form a foundational contribution of this study. However, several limitations constrain the confidence and generalisability of the results.

The study is primarily grounded in a literature review, drawing on academic, doctrinal, and governmental sources. As such, while the resulting framework is well-structured and logically derived, its conclusions are based on moderate confidence levels. The absence of validation through practitioner feedback or live operational contexts limits the certainty with which the proposed competencies can be applied across NATO or national-level OCO planning environments.

Moreover, the availability of peer-reviewed literature explicitly focused on operational-level OCO planning remains limited. Much of the accessible material comes from not formally published and classified government documents, which restricts the transparency and verifiability of specific insights. These constraints are further exacerbated by the classified and sensitive nature of COs, which inherently limit open-source access to operational-level data.

The proposed framework would benefit from further validation through structured expert interviews, live exercise feedback, and cross-case comparisons. These methods are addressed in Publication IV, which extends the current study with expert input and real-world validation steps. Despite its limitations, the current work provides a valuable conceptual baseline for identifying and structuring the core digital, operational, and cognitive skills required by OCO planners. It also lays the groundwork for developing tailored training, certification, and career development pathways for these roles within NATO and partner nations.

5.2 Importance of Planning and Situational Awareness in COs

Modern COs occur in a dynamic, rapidly evolving operational environment, where maintaining robust operational planning and situational awareness is critical for success. As noted by the RAND Corporation, the increasing complexity of contemporary warfare—shaped by persistent technological advancements and the proliferation of sophisticated cyber threats—necessitates continuous adaptation of operational strategies, methodologies, and training programs [135].

One of the key findings of this research is the need to integrate cyberspace operations into multi-domain operational frameworks. The overlapping nature of cyber, land, sea, air, and space operations demands coherent and synchronised operational planning to ensure mission success. This has been corroborated by NATO doctrine, which emphasises the operational imperative of integrating cyberspace capabilities into broader mission execution plans [153].

The cumulative work presented in this thesis has validated this requirement through exercises and operational analysis, particularly by demonstrating how the absence of integrated cyber considerations impedes situational awareness and effective decision-making at the operational and strategic levels.

5.3 The Role of Modelling, Simulation, and Visualisation Frameworks

The research undertaken in this thesis confirms that operational visualisation tools and enhanced cyber situational awareness frameworks are integral to mission success in cyberspace operations [154]. NATO has emphasised that the next generation of modelling and simulation systems must address the challenge of integrating real-time data to provide decision-makers with an integrated, cross-domain operational picture [153]. The Cyber Planner prototype and visualisation tools developed and tested through this research directly respond to this requirement, providing validated use cases in operational exercises.

This conclusion is reinforced by the work of Kookjin et al., who demonstrated the operational importance of a cyber common operational picture framework in achieving situational awareness and enhancing decision-making capabilities during COs [93]. The findings from this research extend these insights by offering empirical validation from large-scale cyber exercises such as Crossed Swords, confirming that cyber planners who utilise enhanced visualisation frameworks are better equipped to anticipate, respond to, and recover from emerging cyber threats.

5.4 Competency Development and Training Frameworks for Cyber Planners

A consistent theme in the literature—and one corroborated through this thesis—is the essential role of structured, competency-based training frameworks in preparing personnel for the complexities of cyberspace operations. The U.S. Army Cyber Centre of Excellence [138], the National Defence University [136], and specialised programs like the Army Information Operations Planners' Course (AIOPC) [137] have all emphasised the need for integrated training approaches that blend technical skills with operational and strategic awareness.

This thesis contributes novel insights into this area by defining individual and organisational competencies required for COs and validating these through operational exercises. The importance of building a curriculum that progresses from foundational technical training to advanced operational planning competencies aligns with best practices in cyber force development. This was further supported by CAPSTONE and other senior-level training courses delivered by the National Defence University [147], which have demonstrated the operational benefits of equipping military leaders with the skills to integrate cyber capabilities into joint, multi-domain operations.

5.5 Integrating Standardised Planning Tools and Frameworks

Another central theme emerging from this research is the need for standardised tools and frameworks to guide cyber operational planning. Integrating established tools such as the ATT&CK Matrix for Enterprise [42] into operational workflows has proven invaluable for structuring, coordinating, and synchronising cyberspace operations. These

tools not only provide a common lexicon for cyber operators but also enable interoperability with multi-domain planning systems.

The cumulative research in this thesis has demonstrated the operational benefits of incorporating such frameworks within cyber exercises, particularly by addressing gaps in operational planning standardisation identified during events such as Crossed Swords. This aligns closely with the objectives outlined by the U.S. Army Cyber Centre of Excellence [138] and the LandCyber White Paper [148], which advocate for a cohesive and interoperable cyber planning capability that can integrate seamlessly with land, air, and maritime operations. The empirical data collected in this thesis supports these doctrinal aims, offering concrete recommendations for operationalising these tools in practice.

5.6 Advancing Organisational Structures and Cyber Force Readiness

The final theme addressed in this discussion concerns the organisational structures and institutional readiness required to support effective cyberspace operations. While initiatives such as those funded by the European Defence Fund continue to advance cyber defence technology capabilities, this research has shown that organisational integration remains a critical enabler for operational success [155].

The integration of COs teams within existing operational headquarters structures—as observed in multiple exercises and validated through scenario testing in this thesis—enhances decision-making speed, improves cross-domain coordination, and ensures more effective alignment of cyber and traditional military operations. This reflects doctrinal recommendations from NATO [10] and the U.S. Army [24], and the cumulative evidence presented in this research offers applied, operational validation for such organisational models.

Furthermore, this thesis highlights the operational value of continuous research and prototyping in improving both cyber defence technologies and command-and-control structures. By embedding research insights into exercise design and operational scenarios, this work has contributed to closing the gap between doctrine and operational practice, a critical issue noted in recent COs literature.

In summary, this chapter has discussed the cumulative findings of this thesis across five thematic areas: the growing importance of operational planning and situational awareness, the role of modelling and simulation frameworks, competency development for cyber planners, the integration of standardised planning tools, and advancing organisational readiness. Each theme has been critically examined in existing literature and doctrine, with operational validation drawn from exercises and prototype testing.

The work demonstrates a profound and nuanced understanding of the challenges and opportunities that modern COs present. To help military practitioners and academic scholars enhance operational planning and situational awareness for commanders, it has provided fresh empirical insights, operational frameworks, and recommendations. These results provide a starting point for additional investigation, practical testing, and doctrinal advancement in this increasingly important field.

5.7 Limitations

Although this thesis offers insightful information about the organisational structures, operational planning tools, and competencies for COs in NATO exercise contexts, several limitations should be noted.

The CS exercise and NATO-affiliated training courses were examples of controlled exercise situations in which most of the data was collected. While these environments mimic operationally relevant situations, results might not apply entirely to OCO in the real world, where strategic, geopolitical, and legal factors introduce additional complexity.

Due to operational security constraints, the study only used unclassified data, literature, and interviews. This limited the ability to capture tactical and operational behaviours specific to classified mission situations, even allowing for broader participation and dissemination.

The empirical components, which included surveys and semi-structured interviews, focused on subject-matter experts from NATO member states and partner organisations. Although the survey's validity was improved by including 22 international respondents who represented various countries' viewpoints, selection bias may be introduced due to the limited sample size.

The study prioritised operational planning tools and Cyber Headquarters, Red Team, and Blue Team structures in exercise settings. It did not cover real-world OCO team structures when life-threatening situations, mission impact, and strategic ramifications greatly affect planning and execution.

Future research should expand the study to include Joint, Combined, and multi-domain planning considerations and attempt to validate these findings in operational contexts, including classified environments.

6 Conclusions and Future Work

This doctoral thesis explored how to improve the planning, execution, and operational effectiveness of CO in military contexts, with a specific focus on OCO. Through a combination of qualitative, quantitative, and experimental research methods—including literature reviews, expert interviews, surveys, and multinational exercise case studies—the study produced operationally validated frameworks and models. These address long-standing doctrinal and organisational gaps within NATO and allied cyber forces.

Three principal research questions guided the research, and the findings are synthesised as follows:

RQ1: What competencies are required for OCO planners?

The research identified and validated a comprehensive framework of competencies essential for OCO planners. These extend beyond technical proficiency to include operational decision-making, risk assessment, adversary emulation, cross-domain integration, and mission command understanding. Publication IV specifically proposed a structured training pathway combining cyber warfare courses, simulated attacks, incident troubleshooting, and risk management, supported by operational planning exercises. This competency framework ensures that planners are prepared to manage COs across the tactical, operational, and strategic levels, bridging a gap previously underrepresented in CO doctrine.

RQ2: What should the optimal organisational structure be for Cyberspace Operations?

The thesis produced three evidence-based, mission-validated frameworks for cyber team structures:

- Cyber Command Headquarters (CHQ), designed with a modular, tailorable structure integrating operational command, technical coordination, and cyber intelligence functions.
- Red Teams, optimised through a central leadership cell with specialist offensive sub-teams responsible for areas such as access operations, effects delivery, and mission reporting.
- Blue Teams, ideally composed of approximately 55 personnel structured into 11 operational elements, based on analysis of historically effective exercise teams.

These structures address doctrinal ambiguity in current NATO planning frameworks and provide a scalable, adaptable template for future exercises and operations.

RQ3: How can operational planning and situational awareness for cyberspace operations be enhanced?

The research demonstrated that effective CO planning requires not only doctrinal frameworks but also enabling technical environments, including distributed ICT infrastructure, advanced visualisation and simulation tools, and interoperable operational planning systems. Publications IV and V outlined how integrating tools such as the ATT&CK Matrix for Enterprise, cyber Common Operational Picture (COP) frameworks, and NATO-standard symbology can enhance real-time situational awareness at all cyberspace layers. The research also proposed the development of advanced decision-support and visualisation systems tailored for the logical layer, addressing a persistent operational challenge. Furthermore, validated training frameworks and competency development models support the sustainable improvement of situational awareness capabilities.

This thesis developed a competency framework for OCO planners, evidence-based organizational structures for CHQ, Red Teams, and Blue Teams, a situational awareness enhancement concept using enhanced symbology and operational visualisation tools. A structured training framework for CO operational planners, linking competencies to practical decision-making scenarios.

By combining qualitative, quantitative, and experimental approaches, this thesis ensured that its theoretical insights are both operationally relevant and scientifically robust. The validity and reliability of the findings were reinforced through methodological triangulation, which was achieved through a literature review, expert interviews, survey validation, and exercise-derived data. Academic rigour influenced research design, data analysis, and the creation of empirically supported frameworks, even if operational applicability was a primary concern. As a result, our study enhances academic knowledge of CO planning, team organisation, and situational awareness in addition to NATO's operational readiness.

This research presents a comprehensive, evidence-based approach to structuring, staffing, and supporting COs in exercise environments. It bridges a persistent gap between theoretical concepts and operational realities in CO planning and execution. The findings provide doctrinally applicable models and recommendations for NATO and allied cyber forces, supporting future exercises, capability development, and doctrinal refinement.

By synthesising insights from literature, expert interviews, operational exercises, and survey-based validation, the thesis advances both theoretical understanding and practical application in the field of COs. It directly contributes to enhancing multinational cooperation, operational decision-making, and cyber mission success in complex, multi-domain conflict environments.

Future work

This study has highlighted areas that need more research and focuses on enhancing operational planning for COs. Building on these results, future studies should thoroughly analyse the operational planning process at all organisational levels whilst considering time restraints, decision-making cycles, and cyberspace's particular difficulties. Furthering this discipline will also involve improving research themes and sub-questions and assessing current frameworks, tools, and processes.

Cyber Planner Tools integration and process assistance will be investigated in stages, such as mission analysis, course of action development, and decision-making. Emerging technologies, such as digital twins and AI-driven decision support, should be assessed for their potential to improve CO planning. Compelling visualisations that will enhance situational awareness and decision-making will be created through user-centred design research. Although this thesis offers a conceptual improvement and a set of user-driven requirements for a Cyber Planner Tool, it has not yet been subjected to a controlled comparative analysis. The systematic validation techniques that should be the focus of future study include controlled trials, comparisons between CHQs, and time-to-decision measurements in exercises such as CS. Compared to present methods, these would aid in determining whether the suggested tool improves situational awareness and planning effectiveness. Investigating alternate design strategies and executing usability tests would provide a wider foundation for evaluating the tool's operational relevance and spotting possible enhancements.

Case studies and empirical validation will assess the usefulness of the suggested tools in practical exercises or operational settings. Cross-domain and multi-domain integration

would determine how CO planning can be included in Multi-Domain Operations to improve cross-domain situational awareness and decision-making.

The author was involved in several European cyberspace operations-related grant projects, such as the European Defence Fund Call EDF-2022-DA-C4ISR-EC2 [156]. The author has contributed to implementing the findings from this thesis into the EC2 project, focusing on enhancing cyber activities such as the Recognised Cyber Picture, rapid defensive response, and cyber risk management within the broader framework of European command and control operations.

The author was a member of the developing consortium EDF-2024-DA-CYBER-NGCR-STEP: Next-Generation Cooperative Cyber Range [157]. This project also involves CO planning, addressing the challenges of large-scale technical cyber exercises, which often need more comprehensive coverage of COs. These exercises require diverse scenarios, environments, and frameworks for operation planning, legal considerations, intelligence activities, and cyber incident management. Key focus areas include analysing cyber operator performance and scoring cybersecurity situational awareness. The author serves as the lead expert in developing the COs theme for this project. The thesis's findings will be integrated into the project to enhance cyber exercise planning, execution, human aspects, and cyberspace situational awareness. This will address challenges in large-scale technical cyber exercises. This project is the most suitable for creating a functional prototype of the proposed Cyber Planner tool, to reach Level Five in Technology Readiness. This involves rigorous validation, risk management, logical connection refinement, and physical layer integration, enhancing allied forces' cyber readiness.

A further project is the Resilient Digital Waterborne Systems for Increased Automation in Smart Shipping (ReDineSS) [158]. The ReDineSS project aims to enhance safety and cybersecurity in the maritime domain by improving situational awareness for human operators and autonomous vessels to ensure data integrity. The author, a cyberspace-activity researcher, contributes to the project by incorporating the findings from their current thesis. This includes the visualisation techniques developed for the Cyber Planner Tool. These techniques enhance operational situational awareness by providing dynamic, intuitive views of cyber terrains and logical connections, which can be effectively adapted to maritime cybersecurity challenges.

Together, these improve operational effectiveness through technology integration, improve tactical decision-making, lessen soldier burden, and implement cybersecurity for mission information integrity. The author has also worked on Project Achille [159]. This will enhance the Next Generation Soldiers Systems' cybersecurity procedures, guaranteeing mission information integrity and operational efficacy.

Although this study offers a solid basis for improving situational awareness and operational planning in COs, more effort is needed to apply its conclusions to military drills and doctrine development. Insights from expert interviews and verified user requirements will help shape the future of NATO CCDCOE-led research projects and exercises, such as creating the Cyber Commanders Handbook and the next edition of AJP-3.20 (Allied Joint Doctrine for Cyberspace Operations).

List of Figures

List of Tables

References

[1] Arik et. al, "Competencies Required for the Offensive Cyber Operations Planners," *HCI for Cybersecurity, Privacy and Trust,* vol. 14729, pp. 20–39, 2024.

[2] Arik, et al., "Optimizing offensive cyber operation planner's development: exploring tailored training paths and framework evolution," *Frontiers in Computer Science,* Vols. Volume 6 - 2024, no. 1400360, 2024.

[3] Arik, et al., "Enhancing Operational Planning and Situational Awareness for Cyberspace Operations," *European Conference on Cyber Warfare and Security (ECCWS),* vol. 24.1, no. 1, p. 3327–3337, 2025.

[4] AKIT, "AKIT," 11 September 2024. [Online]. Available: https://akit.cyber.ee/term/1170-blue-team. [Accessed 15 July 2025].

[5] D. Barber, A. Bobo and K. Sturm, "Cyberspace Operations Planning: Operating a Technical Military," *Military Cyber Affairs,* vol. 3, no. 1, pp. Volume 1, Issue 1, Article 3, page 6., 2016.

[6] M. Arik, A. Venables and R. Ottis, "Planning Cyberspace Operations: Exercise Crossed Swords Case Study," *Journal of Information Warfare,* pp. 67–78, Vol. 21, No. 4 Fall 2022.

[7] M. Arik, R. G. Lugo, R. Ottis and A. N. Venables, "Optimizing offensive cyber operation planner's development: exploring tailored training paths and framework evolution," *Front. Comput. Sci., 07 June 2024,* vol. 6, no. https://doi.org/10.3389/fcomp.2024.1400360, pp. 1456-1465, 07 June 2024.

[8] CCDCOE, "Locked Shields," 10 September 2024. [Online]. Available: https://ccdcoe.org/exercises/locked-shields/.

[9] CCDCOE, "Crossed Swords," The NATO Cooperative Cyber Defence Centre of Excellence, 15 June 2023. [Online]. Available: https://ccdcoe.org/exercises/crossed-swords/. [Accessed 15 June 2023].

[10] CCDCOE, "TRUST IN CYBER EXERCISES: A VISION FOR NATO," 07 March 2022. [Online]. Available: https://ccdcoe.org/uploads/2022/07/Trust-in-Cyber-Exercises-March-2022.pdf. [Accessed 07 March 2025].

[11] U.S. Naval Institute, "U.S. Naval Institute," June 2018. [Online]. Available: https://www.usni.org/magazines/proceedings/2018/june/focus-offensive-cyberspace-operations. [Accessed 07 March 2025].

[12] J. Doubleday, "Will 2024 bring some resolutions for the cyber workforce problem?," Federal News Network, 25 December 2023. [Online]. Available: https://federalnewsnetwork.com/federal-report/2023/12/wil-2024-bring-some-resolutions-for-the-cyber-workforce-problem/. [Accessed 07 March 2025].

[13] M. Hill, "Cybersecurity workforce shortage reaches 4 million despite significant recruitment drive," 31 October 2023. [Online]. Available: https://www.csoonline.com/article/657598/cybersecurity-workforce-shortage-reaches-4-million-despite-significant-recruitment-drive.html. [Accessed 07 March 2025].

[14] (ISC)2, “CYBERSECURITY WORKFORCE STUDY,” 18 October 2022. [Online]. Available: https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf.

[15] IISS, “GREAT-POWER OFFENSIVE CYBER CAMPAIGNS:Experiments in Strategy,” The International Institute for Strategic Studies, London, 2022.

[16] M. Smeets, “The challenges of military adaptation to the cyber domain: a case study of the Netherlands,” *SMALL WARS & INSURGENCIES,* p. 1343–1362, 2023.

[17] Stephanie Pendino et al., “U.S. Cyber Deterrence: Bringing Offensive Capabilities into the Light,” *The Journal of the Joint Forces Staff College,* pp. 1–10, 2022.

[18] RAND Corporation, “Operationalizing Cyberspace as a Military Domain,” RAND Corporation, Santa Monica, 2019.

[19] Lorenzo Neil et. al, “Analyzing Cybersecurity Definitions for Non-experts,” in *FIP International Symposium on Human Aspects of Information Security & Assurance (HAISA 2023)*, Kent, GB, 2023.

[20] Mariana G. Cains et al., “Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation,” *Risk Analysis, Vol. 42, No. 8, 2022,* vol. 42, no. 8, pp. 1–27, 2022.

[21] S. Adam, “The Impact of Organizational Structure on Cybersecurity Outcomes,” 05 March 2024. [Online]. Available: https://news.sophos.com/en-us/2024/03/05/the-impact-of-organizational-structure-on-cybersecurity-outcomes/.

[22] Compyl, “Cybersecurity Organizational Structure,” 10 August 2023. [Online]. Available: https://compyl.com/blog/cybersecurity-organizational-structure/.

[23] Joint Chiefs of Staff, “Public Intelligence,” 2018 July 2018. [Online]. Available: https://publicintelligence.net/jcs-cyberspace-operations/. [Accessed 04 March 2025].

[24] U.S. Air Force, “Air Force Doctrine Publication 3-12 - Cyberspace Operations,” 01 February 2023. [Online]. Available: https://www.doctrine.af.mil/Doctrine-Publications/AFDP-3-12-Cyberspace-Ops/.

[25] AJP-3.20, “ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS,” January 2020. [Online]. Available: https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320.

[26] Gazmend Huskaj, et al., “A Theory of Offensive Cyberspace Operations and Its Policy and Strategy Implications,” in *Proceedings of the 23rd European Conference on Cyber Warfare and Security, ECCWS 2024*, Jyvasküla, 2024.

[27] M. S. Lund, “HYBRID THREATS IN CYBERSPACE,” in *Preparing for Hybrid Threats to Security*, London, Routledge, 2024, p. 15.

[28] NATO, 09 July 2016. [Online]. Available: https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[29] S. v. d. Meer, “The need for balancing offensive and defensive cyber operations,” Netherlands Instititue of International Relations, The Hague, 2019.

[30] J. E. McGhee, “Liberating Cyber Offense,” *Strategic Studies Quarterly, Winter 2016,* pp. 46–63, 2016.

[31] J. Skingsley, “Offensive cyber operations States perceptions of their utility and risks,” Chatham House, London, 2023.

[32] C. Bailey, “OFFENSIVE CYBERSPACE OPERATIONS: A GRAY AREA IN CONGRESSIONAL OVERSIGHT,” *BOSTON UNIVERSITY INTERNATIONAL LAW JOURNAL Vol. 38:2,* pp. 240–285, 2020.

[33] M. Smeets, “The Strategic Promise of Offensive Cyber Operations,” *Strategic Studies Quarterly ♦ Fall 2018,* pp. 90–113, 2018.

[34] F. Hanson and T. Uren, “ORGANISATION, COMMAND AND APPROVALS,” JSTOR, New York, 2018.

[35] M. S. Jensen, “Five good reasons for NATO’s pragmatic approach,” *Defence Studies,* pp. 464–488, 2022.

[36] Joint Publication 5-0, “Doctrine for Planning Joint Operations,” 13 April 1995. [Online]. Available: https://edocs.nps.edu/dodpubs/topic/jointpubs/JP5/JP5-0_950413.pdf.

[37] Joint Doctrine Publication 0-01, “UK Defence Doctrine,” November 2022. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1118720/UK_Defence_Doctrine_Ed6.pdf.

[38] Joint Publication 1, “Joint Publication 1 Volume 1,” 27 August 2023. [Online]. Available: https://keystone.ndu.edu/Portals/86/Joint%20Warfighting.pdf.

[39] NSO, “Allied Joint Doctrine for the Planning of Operations (AJP-5),” May 2019. [Online]. Available: https://www.gov.uk/government/publications/allied-joint-publication-ajp-05a-allied-joint-doctrine-for-the-planning-of-operations.

[40] NATO Defense College, “NATO’s needed offensive cyber capabilities,” 29 May 2020. [Online]. Available: https://www.ndc.nato.int/news/news.php?icode=1441#_edn1.

[41] A. Dalmijn, V. Banse, L. Lumiste, J. Teixeira and A. B. (Eds.), Cyber Commander’ Handbook, Tallinn: NATO CCDCOE Publications, 2020.

[42] MITRE, “ATT&CK,” The MITRE Corporation, 09 OKT 2024. [Online]. Available: https://attack.mitre.org/.

[43] UK Ministry of Defence, “Allied Joint Publications (AJPs),” 11 October 2024. [Online]. Available: https://www.gov.uk/government/collections/allied-joint-publication-ajp. [Accessed 20 Feb 2025].

[44] T. Boos, “Geographies of Cyberspace: Internet, Community, Space, and Place. In Inhabiting Cyberspace and Emerging Cyberplaces,” *Geographies of Media,* pp. 13–38, 2017.

[45] Ministry of Defence, “Guidance,” 4 October 2022. [Online]. Available: https://www.gov.uk/government/publications/cyber-primer. [Accessed 18 Feb 2025].

[46] Lawfare, “Cyber Command’s Strategy Risks Friction With Allies,” 28 May 2019. [Online]. Available: https://www.lawfaremedia.org/article/cyber-commands-strategy-risks-friction-allies. [Accessed 18 Feb 2025].

[47] J.-P. CHRISTOPHE, 08 Jan 2020. [Online]. Available: https://apps.dtic.mil/sti/trecms/pdf/AD1177547.pdf. [Accessed 04 March 2025].

[48] Adrian Venables et. al, "A Model for Characterizing Cyberpower," in *9th International Conference on Critical Infrastructure Protection*, Arlington, 2015.

[49] Venables, A, "Modelling Cyberspace to Determine Cybersecurity Training Requirements," *Frontiers in Education,* pp. 1–16, 2021.

[50] Grandin, "Cyberspace Geography and Cyber Terrain: Challenges in Producing a Universal map of Cyberspace," in *Proceedings of the 22nd European Conference on Cyber Warfare and Security, ECCWS 2023*, Piraeus, 2023.

[51] Army Techniques Publication, "ATP 2-01.3, Intelligence Preparation of the Battlefield,Change No. 2, No. 2-01.3," Washington, 2024.

[52] Army Techniques Publication, "ATP 2-01.3, Intelligence Preparation of the Battlefield," Washington, 2019.

[53] Ministry of Defence, "Cyber and Electromagnetic Activities (JDN 1/18)," June 27 2024. [Online]. Available: https://www.gov.uk/government/publications/cyber-and-electromagnetic-activities-jdn-118. [Accessed 19 Feb 2025].

[54] Department of the Army, "Cyberspace and Electronic Warfare Operations, April 2017. Unclassified," 1 April 2017. [Online]. Available: https://nsarchive.gwu.edu/document/22844-document-11-department-army-fm-3-12. [Accessed 04 March 2025].

[55] Army Publishing Directorate , "Intelligence Resource Program," August 2021. [Online]. Available: https://irp.fas.org/doddir/army/fm3-12.pdf. [Accessed 19 Feb 2025].

[56] M. Arik, "How Do NATO Members Define Cyber Operations?," in *International Conference on Human-Computer Interaction*, Copenhagen, 2023.

[57] K. Kaska and L. Aasmann, "Julgeolekuasutuste roll küberjulgeoleku tagamisel ja seda mõjutavad suundumused rahvusvahelises õiguses," 2020. [Online]. Available: https://juridica.ee/article.php?uri=2020_2_julgeolekuasutuste_roll_k_berjulgeoleku_tagamisel_ja_seda_m_jutavad_suundumused_rahvusvahelis. [Accessed 20 July 2025].

[58] Robert Janczewski et al., "Terminology as a Barrier to NATO's Interoperability in Cyberspace Operations," in *International conference KNOWLEDGE-BASED ORGANIZATION*, Warsaw, 2019.

[59] Belfer Center for Science and International Affairs John F. Kennedy School of Government, "National Cyber Power Index 2020," September 2020. [Online]. Available: https://www.belfercenter.org/publication/national-cyber-power-index-2020. [Accessed 15 June 2023].

[60] V. LaPiana and N. Richmond, "TERRAIN IN CYBERSPACE OPERATIONS—," CARNEGIE MELLON UNIVERSITY, Pittsburgh, 2024.

[61] Modern War Institute, "Pressing Questions: Offensive Cyber Operations and NATO Strategy," 25 Jan 2022. [Online]. Available: https://mwi.westpoint.edu/pressing-questions-offensive-cyber-operations-and-nato-strategy/. [Accessed 08 July 2025].

[62] M. S. Jensen, “Offensive Cyber Capabilities and Alliances,” Syddansk Universitet, Syddansk, 2023.

[63] The Cyber Signal, “Offensive Cyber Operations: A National Security Imperative,” 29 Jun 2023. [Online]. Available: https://www.afcea.org/signal-media/cyber-edge/offensive-cyber-operations-national-security-imperative. [Accessed 04 March 2025].

[64] FBI, “FBI,” FBI National Press Office, 30 May 2024. [Online]. Available: https://www.fbi.gov/news/press-releases/operation-endgame-coordinated-worldwide-law-enforcement-action-against-network-of-cybercriminals. [Accessed 04 March 2025].

[65] Joint Forces Staff College, “Academic Journals | Sept. 7, 2022,” Academic Journals, 07 Sept 2022. [Online]. Available: https://jfsc.ndu.edu/Media/Campaigning-Journals/Academic-Journals-View/Article/3149856/us-cyber-deterrence-bringing-offensive-capabilities-into-the-light/. [Accessed 04 March 2025].

[66] W. Goździewicz, “Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA),” 11 November 2019. [Online]. Available: https://www.cyberdefensemagazine.com/sovereign-cyber/.

[67] M. N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Rhode Island: Cambridge University Press, 2017.

[68] M. J. Weiskopff, “Effects-Based Operations in the Cyber Domain,” Viewed 4 September 2024 2017. [Online]. Available: https://apps.dtic.mil/sti/citations/AD1033006.

[69] Allied Joint Publication , “Allied Joint Publication-3.20,” January 2020. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

[70] D. T. Long, “Wargaming and the Education Gap: Why CyberWar: 2025 Was Created,” *The Cyber Defense Review,* pp. 185-198, Spring 2020.

[71] RAND Corporation, “Wargaming,” RAND, 25 Jan 2025. [Online]. Available: https://www.rand.org/topics/wargaming.html. [Accessed 25 Feb 2025].

[72] NATO CCDCOE, “CCDCOE,” 12 Feb 2025. [Online]. Available: https://ccdcoe.org/. [Accessed 19 Feb 2025].

[73] NATO CCDCOE, “Locked Shields,” 04 March 2025. [Online]. Available: https://ccdcoe.org/exercises/locked-shields/. [Accessed 04 March 2025].

[74] AKIT, “blue team,” 19 Feb 2025. [Online]. Available: https://akit.cyber.ee/term/1170-blue-team. [Accessed 19 Feb 2025].

[75] J. M. &. T. B. Pullen, “Visual planning for cyber operations,” in *Cyber Operations: Building, Defending, and Attacking Modern Computer Networks*, Towson, Apress., 2015, pp. 221-239.

[76] D. D. Suthers, “Technology affordances for intersubjective meaning making: A research agenda for CSCL.,” *Computer Supported Learning 1,* p. 315–337, 2006.

[77] Paul Barford et.al., “Cyber SA: Situational Awareness for Cyber Defense,” *In Cyber Situational Awareness,* pp. 3–14, 2010.

[78] G. B. Dobson and K. M. Carley, “Cyber-FIT Agent-Based Simulation Framework Version 4,” Center for the Computational Analysis of Social and Organizational Systems, Pittsburgh, 2021.

[79] M. R. Endsley, “Toward a Theory of Situation Awareness in Dynamic Systems,” *The Journal of the Human Factors and Ergonomics Society, 37(1),* p. 32–64, 1995.

[80] NIST, “A Role-Based Model for Federal Information Technology/Cybersecurity Training,” U.S. Department of Commerce, Virginia, 2014.

[81] E. D. McCroskey and C. A. Mock, “Operational Graphics for Cyberspace,” *Joint Force Quarterly 85,* p. 43, 2017.

[82] Liuyue Jiang et al., “Systematic Literature Review on Cyber Situational Awareness Visualizations,” *IEEE Access, vol. 10,* pp. 57525–57554, 2022.

[83] U. Franke and J. Brynielsson, “Cyber situational awareness—A systematic review of the literature,” *Computers & Security, 46,* pp. 18–31, 2014.

[84] K. Renaud and J. Ophof, “An SME-specific cyber situational awareness model to predict the implementation of cybersecurity practices,” *Journal of Cybersecurity,* pp. 24–46, 2021.

[85] T. F. Ask, K. Kullmann, S. Sütterlin, B. Kox, D. Engel and R. Lugo, “A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness,” *Sec. Cybersecurity and Privacy,* vol. 6, pp. Online Volume 6 - 2023 | https://doi.org/10.3389/fdata.2023.1042783, 2023.

[86] NATO, “NATO - STANAG 2019 NATO JOINT MILITARY SYMBOLOGY,” 23 Feb 2024. [Online]. Available: https://standards.globalspec.com/std/10266440/STANAG%202019.

[87] NSO, “NATO STANDARD APP-06 NATO JOINT MILITARY SYMBOLOGY,” NATO STANDARDIZATION OFFICE (NSO), Brussels, 2023.

[88] TRADOC G–2 , THE RED TEAM HANDBOOK, FT Leavenworth, KS: University of Foreign Military and Cultural Studies TRADOC G-2 Intelligence Support Activity, 2022.

[89] J. Kick, Cyber Exercise Playbook, Wiesbaden: MITRE, 2014.

[90] J. T. Joe Vest, Red Team Development and Operations: A Practical Guide, Independently published, 2020.

[91] A. WHITE and B. LARK, BTMF Blue Team Field Manual, Worldwide: CreateSpace Publishing, 2017.

[92] Arik et al., “The Optimal Organisational Structure for Cyber Operations based on exercise lessons,” in *European Conference on Cyber Warfare and Security 23(1):*37–48, Jyväskylä, 2024.

[93] Kookjin et.al, “Study on Cyber Common Operational Picture Framework for Cyber Situational Awareness,” *Applied Sciences,* p. https://doi.org/10.3390/app13042331, 2023.

[94] Wang et. al., “CYBERSPACE MAP MODEL CREATION METHOD AND DEVICE,” Patent Application Publication, Houston, 2021.

[95] Wong et. al., “A Framework for Measuring Situation Awareness in Cyberspace Operations,” *Proceedings of the Human Factors and Ergonomics Society Annual MeetingVolume 65, Issue 1,* pp. 358–362, 2021.

[96] Mock and McCroskey, “Operational Graphics for,” *Joint Force Quarterly 85,* pp. Online [https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1130660/operational-graphics-for-cyberspace/], 1 April 2017.

[97] Innovation Development Institute, “Argos - Visualization Tool for Cyberspace Command and Control,” 2009. [Online]. Available: https://www.inknowvation.com/sbir/awards/af-2009-argos-visualization-tool-cyberspace-command-and-control.

[98] Hasan et. al, “A Cyberspace Effects Server for LVC&G Training Systems,” in *2021 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC)*, Orlando, 2021.

[99] V. L. P. C. John W. Creswell, Designing and Conducting Mixed Methods Research, Los Angeles: SAGE Publications, 2017.

[100] European Commission, “European e-Competence Framework,” European Commission, 15 May 2024. [Online]. Available: https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf. [Accessed 15 July 2025].

[101] Moher et al., “Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement,” *Systematic reviews,* pp. 1–9, 2015.

[102] Tricco et al., “PRISMA Extension for Scoping Reviews (PRISMA-ScR): Checklist and Explanation,” *Annals of Internal Medicine,* pp. 467–473, 2018.

[103] S. J. Tracy, “Qualitative Quality: Eight “Big-Tent” Criteria for Excellent Qualitative Research,” *Qualitative inquiry, 16(10),* pp. 837–851, 2010.

[104] L. Kosmol and C. Leyh, “ICT Usage in Industrial Symbiosis: Problem Identification and Study Design,” 2019. [Online]. Available: https://annals-csis.org/proceedings/2019/drp/pdf/323.pdf.

[105] Peffers et al., “A design science research methodology for information systems research,” *Journal of Management Information Systems 24,* vol. 24, no. 3, pp. 45–77, 2007.

[106] B. Kitchenham and S. M. Charters, “Guidelines for performing Systematic Literature Reviews in Software Engineering,” EBSE Technical Report, EBSE-2007-01, Durham, 2007.

[107] M. Pomerleau, “More expertise may be needed for military commands to call for non-kinetic capabilities,” 14 FEb 2024. [Online]. Available: https://defensescoop.com/2024/02/14/expertise-non-kinetic-capabilities-resident-military-commands/.

[108] H. Singh, “The Tribune,” 02 Dec 2024. [Online]. Available: https://www.tribuneindia.com/news/defence/multi-domain-operations-are-the-future/. [Accessed 02 Dec 2024].

[109] NICCS, “Cyber Operational Planning,” 30 October 2023. [Online]. Available: https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/cyber-operational-planning.

[110] NICCS, “Cyber Operations Planning,” National Initiative for Cybersecurity Careers and Studies, Nov 2020. [Online]. Available: https://niccs.cisa.gov/workforce-development/nice-framework/work-role/cyber-operations-planning. [Accessed 25 Feb 2025].

[111] A. J. Curnutt and S. R. Sikes, “NAVAL POSTGRADUATE SCHOOL,” September 2021. [Online]. Available: https://apps.dtic.mil/sti/citations/AD1164246.

[112] R. Houston, *Thriving Cybersecurity Professionals:Building a Resilient Workforce and Psychological Safety in the Federal Government,* Pennsylvania: University of Pennsylvania, 2019.

[113] U.S. General Services Administration, “U.S. General Services Administration,” 01 September 2022. [Online]. Available: https://www.gsaadvantage.gov/ref_text/47QTCA22D00C8/0XKGIE.3TATEZ_47QTCA22D00C8_NNDATA47QTCA22D00C8A81509012022.PDF.

[114] NATO CCDCOE, “NATO CCDCOE,” September 2023. [Online]. Available: https://ccdcoe.org/uploads/2023/09/2023_NATO_CCD_COE_Training_Catalogue_final.pdf.

[115] Lockheed Martin, “Lockheed Martin,” 04 May 2023. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

[116] Rand Corporation, “A Cost Estimating Framework for U.S. Marine Corps Joint Cyber Weapons.,” RAND Corporation. For more information on this publication, visit www.rand.org/t/RRA1124-1., Santa Monica, 2023.

[117] Navy Personnel Command, “CHAPTER 20 CRYPTOLOGIC TECHNICIAN (NETWORKS) (CTN),” July 2023. [Online]. Available: https://www.mynavyhr.navy.mil/Portals/55/Reference/NEOCS/Vol1/CTN_occs_CH_95_Jul23.pdf?ver=CWQ8uOEoG-z0c7PLZqXKRg%3d%3d.

[118] M. Arik, “Google Drive,” 21 Dec 2024. [Online]. Available: Appendix 1 – The Framework for Offensive Cyber Operations Planners.. [Accessed 21 Feb 2025].

[119] Chowdhury and Gkioulos, “Key competencies for critical infrastructure cyber-security: A systematic literature review.,” *Information & Computer Security,* pp. 697-723, 2021.

[120] JOINT STAFF WASHINGTON, D.C. 20318, “METHODOLOGY FOR COMBAT ASSESSMENT,” 8 March 2019. [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/training/jts/cjcsi_3162_02.pdf?ver=2019-03-13-092459-350. [Accessed 25 Feb 2025].

[121] U.S. Air Force, “Air Force Doctrine Publication 3-60,” 12 Nov 2021. [Online]. Available: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-60/3-60-AFDP-TARGETING.pdf. [Accessed 04 March 2025].

[122] M. Nizich, “Emerald insight,” 31 July 2023. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/978-1-80382-915-920231006/full/html.

[123] J. M. Bender, “The Cyberspace Operations Planner,” *Small Wars Journal,* p. 16, 2013.

[124] M. R. Lidestri, “INCORPORATING PERISHABILITY AND OBSOLESCENCE INTO CYBERWEAPON SCHEDULING,” MONTEREY, 2022.

[125] L. A. Mulford, “LET SLIP THE DOGS OF (CYBER) WAR: PROGRESSING TOWARDS A,” Joint Advanced Warfighting School, Norfolk, 2013.

[126] Australian Strategic Policy Institute, “Defining offensive cyber capabilities,” Australian Strategic Policy Institute, 4 July 2018. [Online]. Available: https://www.aspi.org.au/report/defining-offensive-cyber-capabilities. [Accessed 25 Feb 2025].

[127] Neville, Kelly; et al., “United States Army Research Institute for the Behavioral and Social Sciences,” January 2020. [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD1091744.pdf.

[128] NIST GOV, “Situational Awareness a New Way to Attack Cybersecurity Issues Rather Than,” UNK. [Online]. Available: https://www.nist.gov/document/tri-countyelectriccooperativepart2032613pdf. [Accessed 20 Feb 2025].

[129] J. L. Caton, Implications of Service Cyberspace Component Commands for Army Cyberspace Operations, Carlisle: USAWC Press, 2019.

[130] D. Shoemaker, A. Kohnke and K. Sigler, A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0), Florida: CRC Press, 2016.

[131] M. Berman, “What is Digital Technology?,” Programming Insider, 28 October 2021. [Online]. Available: https://programminginsider.com/what-is-digital-technology/. [Accessed 20 Feb 2025].

[132] P. Withers, “Integrating Cyber with Air Power in the Second Century of the Royal Air Force,” *Royal Air Force Air Power Review, 21(3),* pp. 148–151, 2018.

[133] U.S. Department of Defense, “ DevSeccOps Fundamentals Guidebook - U.S. Department of Defense,” 25 May 2023. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DevSecOpsActivitesToolsGuidebookTables.pdf?ver=_Sylg1WJB9K0Jxb2XTvzDQ%3d%3d. [Accessed 21 Feb 2025].

[134] NIST, “NICE Framework Resource Center, Workplace Skills and the NICE Framework,” 1 November 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf. [Accessed 11 11 2025].

[135] RAND Corporation, “Educating for Evolving Operational Domains,” RAND Corporation, California, 2022.

[136] National Defense University, “CAPSTONE,” National Defense University, 25 Feb 2025. [Online]. Available: https://capstone.ndu.edu/Home/Course-Overview/. [Accessed 25 Feb 2025].

[137] Group, 1st Information Operations Command, “Army Information Operations Planners’ Course (AIOPC),” Hosted by Defense Media Activity, 25 Feb 2025. [Online]. Available: https://www.1stio.army.mil/Training/IO-Training/Army-Information-Operations-Planners-Course-AIOPC/. [Accessed 25 Feb 2025].

[138] U.S. Army Cyber Center of Excellence (CCoE), “Cyber School Functional Courses,” U.S. Army Cyber Center of Excellence (CCoE), 25 2025 2025. [Online]. Available: https://cybercoe.army.mil/Cyber-Center-of-Excellence/Schools/Cyber-School/Functional-Courses/. [Accessed 25 Feb 2025].

[139] V. Braun and V. Clarke, “Using thematic analysis in psychology,” *Qualitative Research in Psychology, 3(2),* pp. 77–101, 2006.

[140] U. Flick, From Intuition to Reflexive Construction: Research Design and Triangulation in Grounded Theory Research, SAGE Publications Ltd, 2019, pp. 125–144.

[141] NAVMC, NAVMC 3500.124, DEPARTMENT OF THE NAVY HEADQUARTERS UNITED STATES MARINE CORPS, 2018.

[142] A Lemay et. al, “Intelligence Preparation of the Cyber Environment (IPCE),” *Journal of Information Warfare,* pp. 46–56, 2014.

[143] Salvador Llopis et al., “A comparative analysis of visualisation techniques to achieve cyber situational awareness in the military,” *2018 International Conference on Military Communications and Information Systems (ICMCIS),* pp. 1–7, 2018.

[144] M. Pfannenstiel and D. Cox, “NATO’s Cyber Era (1999–2024) Implications for Multidomain,” *MILITARY REVIEW ONLINE EXCLUSIVE · OCTOBER 2024,* pp. 1–10, 2024.

[145] Department of Defense, “JOINT MILITARY SYMBOLOGY,” 10 June 2014. [Online]. Available: http://everyspec.com/MIL-STD/MIL-STD-2000-2999/MIL-STD-2525D_50933/.

[146] P.-I. Evensen, “Requirements for Simulation of the Future Operating Environment,” in *I/ITSEC 2024 Paper No. 24139*, Orlando, 2024.

[147] Allied Command Transformation, “NATO Allied Command Transformation,” 1 August 2023. [Online]. Available: https://www.act.nato.int/article/nexgen-modelling-and-simulation/. [Accessed 21 Feb 2025].

[148] U.S. ARMY, “THE U.S. ARMY LANDCYBER WHITE PAPER 2018-2030,” U.S. Army Capabilites Integration Center, Fort George G. Meade,, 2013.

[149] W. Bryant, “Mission Assurance through Integrated Cyber Defense,” *Air and Space Power Journal,* pp. 5–18, 2016.

[150] M. Klipstein, “Seeing is Believing: Quantifying,” *THE CYBER DEFENSE REVIEW,* p. 88, 2019.

[151] S. Mohite, “Cybersecurity operations and the role of visualization, design, and usability,” 26 January 2018. [Online]. Available: https://medium.com/uplevel/how-design-visualization-and-usability-impact-cybersecurity-operations-61d854b5e2d3. [Accessed 20 September 2023].

[152] M. Héder, “From NASA to EU:the evolution of the TRL scale in Public Sector Innovation,” *The Innovation Journal: The Public Sector Innovation Journal, Volume 22(2),* vol. Vol. 22, no. No. 2, pp. Article 3, 1-23, 2017.

[153] NATO, “NATO Exercises to Enhance its Cyber Resilience,” 20 November 2023. [Online]. Available: https://www.act.nato.int/article/nato-exercises-to-enhance-its-cyber-defences/. [Accessed 07 March 2025].

[154] Tracy, “Qualitative Quality: Eight “Big-Tent” Criteria for Excellent Qualitative Research,” *Qualitative inquiry, 16(10),* pp. 837-851, 2010.

[155] European Defence Fund, 23 July 2024. [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/edf/wp-call/2024/call-fiche_edf-2024-da_en.pdf.

[156] European Defence Fund, “European Defence Fund (EDF) Call for proposals EDF-2022-DA,” 09 June 2022. [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/edf/wp-call/2022/call-fiche_edf-2022-da_en.pdf. [Accessed 28 Feb 2025].

[157] European Defence Fund, “European Defence Fund (EDF) Call for proposals EDF-2024-DA Call for EDF development actions implemented via actual cost grants,” 28 August 2024. [Online]. Available: https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/edf/wp-call/2024/call-fiche_edf-2024-da_en.pdf. [Accessed 28 Feb 2025].

[158] European Commission, “Ensuring the safety, resilience and security of waterborne digital systems – HORIZON Europe Framework Programme (HORIZON-CL5-2024-D6-01-10),” European Commission, 18 July 2024. [Online]. Available: https://transport.ec.europa.eu/transport-modes/maritime/ship-financing-portal/ensuring-safety-resilience-and-security-waterborne-digital-systems-horizon-europe-framework_en. [Accessed 25 Feb 2025].

[159] Defence Industry Europe, “ACHILE project: Euroepan industry to develop next-generation dismounted soldier systems,” Defence Industry Europe, 14 June 2023. [Online]. Available: https://defence-industry.eu/achile-project-euroepan-industry-to-develop-next-generation-dismounted-soldier-systems/. [Accessed 28 Feb 2025].

Acknowledgements

I want to thank everyone who helped me during my research and express my sincere gratitude to my supervisors, Prof. Rain Ottis and Dr Adrian Nicholas Venables, for their essential support, knowledge, and counsel. Your advice has influenced how I approach my work.

Thank you so much to the NATO CCDCOE and Mr. Carry Kangur for providing me with vital resources for my thesis. As well as the Estonian Defence Forces Cyber Command, for their invaluable cooperation and support in providing necessary resources for this thesis.

Additionally, I appreciate Dr. Cate Jerram's and Dr. Ricardo Lugo's helpful criticism and assistance with this research. Your insights have improved my comprehension of the topic.

In memoriam, I thank Mr. Kim Vahturov for his unwavering encouragement and support during this journey. Your counsel and understanding have motivated me to go through this journey of the mind.

Finally, I thank Talgen Cybersecurity OÜ for partially funding my research and Mr Uko Valtenberg for his aid and counsel.

Every encouragement helps to accomplish the task at hand.

Abstract

The Planning, Development and Execution of Cyber Operations in the Digital Information Environment

As states prepare for multinational joint operations and exercises, CO becomes a more critical field within NATO's armed forces and civilian structures. Unanimity in the stakeholders' knowledge of CO definitions is crucial for success. This thesis addresses the unique features of cyberwarfare and offers a crucial foundation for enhancing CO planning capabilities.

Publication VI of the research elucidates the basic definitions of COs, while Publication I highlights the distinctions between cyber and conventional land-based military operations. CO planners and decision-makers must know these differences as cyber operations frequently call for distinct strategies, tactics, and equipment instead of kinetic operations.

The thesis subsequently explores the skills required by individuals and organisations engaged in CO (Publication III). The first step in creating comprehensive cyber planners is determining the knowledge and skill sets needed to participate in cyber exercises and real-world operations. Furthermore, Publication IV thoroughly validates the suggested training framework for OCO planners, guaranteeing that it aligns with present NATO standards and upcoming operational requirements.

Another important topic covered in the thesis is organisational structure (Publication II). In particular, it provides the best design for OCO, DCO, and CHQ for the CO planning team. This organisational structure ensures that special requirements for cyber operations are satisfied while preserving operational effectiveness at different command levels.

Lastly, the thesis discusses the logical layer of cyberspace, one of the biggest challenges in COs (Publication V). It offers solutions to lessen this layer's difficulties, guaranteeing that planners can successfully negotiate the intricacies of CO planning. These realisations provide the groundwork for creating sophisticated CO planning instruments, speeding up decision-making and improving NATO's cyber forces' operational capacity.

This thesis offers a thorough framework to ensure that NATO's CO planning capabilities are improved and ready for future multinational COs.

Lühikokkuvõte

Küberoperatsioonide planeerimine, arendamine ja läbiviimine digitaalses infokeskkonnas

Küberoperatsioonid on NATO relvajõududes ja tsiviilstruktuurides üha olulisem valdkond, kuna riigid valmistavad oma kübervõimekust ette rahvusvaheliste ühisoperatsioonide ja õppuste jaoks. Edukuse kriitiline eeltingimus on eri huvirühmade ühtne arusaam küberoperatsiooni määratlustest. Käesolev doktoritöö annab olulise raamistiku küberoperatsioonide planeerimisvõimekuse arendamiseks, keskendudes kübersõja ainulaadsete omaduste käsitlemisele.

Uuring selgitab küberruumi operatsioonide põhimääratlusi (väljaanne VI), rõhutades erinevusi küberoperatsioonide ja traditsiooniliste maismaal toimuvate sõjaliste operatsioonide vahel (väljaanne I). Nende erinevuste mõistmine on oluline küberoperatsiooni planeerijate ja otsustajate jaoks, sest küberoperatsioonid nõuavad sageli võrreldes kineetiliste operatsioonidega teistsuguseid lähenemisviise, taktikaid ja vahendeid.

Seejärel käsitletakse käesolevas töös vajalikke pädevusi, mis peavad küberoperatsiooniga seotud üksikisikutel ja meeskondadel olema (III väljaanne). Küberõppustel ja tegelikes operatsioonides tõhusaks osalemiseks vajalike oskuste ja teadmiste kindlaksmääramine annab aluse mitmekülgsete küberplaneerijate arendamiseks. Lisaks on kavandatud väljaõpperaamistik küberründe operatsioonide planeerijatele rangelt kehtiv (IV väljaanne), tagades, et see on kooskõlas praeguste NATO standardite ja tulevaste operatsioonide vajadustega.

Organisatsiooni struktuur on teine kriitiline komponent, mida antud töös uuritakse (II väljaanne). See pakub küberoperatsioonide planeerimispersonalile optimaalse ülesehituse, eelkõige ründavad küberoperatsioonid, kaitsvad küberoperatsioonid ja küberstaabi jaoks. Antud struktuuriline raamistik tagab, et tegevus on kooskõlas küberoperatsiooni ainulaadsete nõudmistega, säilitades samal ajal operatiivse tõhususe erinevatel juhtimistasanditel.

Lõpuks käsitletakse töös ühte kõige keerulisemat väljakutset küberruumi operatsioonides – küberruumi loogilist kihti (V väljaanne). See pakub strateegiaid antud kihiga seotud väljakutsete leevendamiseks, tagades planeerijate tõhusa navigeerimise küberoperatsioonide planeerimise keerukuses. Käesolevad teadmised loovad aluse täiustatud küberoperatsioonide planeerimisvahendite väljatöötamiseks, hõlbustades reaalajas otsuste tegemist ja suurendades NATO kübervägede operatiivvõimekust.

Antud doktoritöö pakub tervikliku raamistiku NATO küberoperatsioonide planeerimisvõime loomiseks ja täiustamiseks, tagades valmisoleku tulevasteks rahvusvahelisteks küberoperatsioonideks.

Appendix 1

Publication I

Arik, Marko; Venables Adrian; Ottis Rain (2022). Planning Cyberspace Operations: Exercise Crossed Swords Case Study. Journal of Information Warfare, 21 (4), 67−78.

Planning Cyberspace Operations: Exercise Crossed Swords Case Study

M Arik, A Venables, R Ottis

Tallinn University of Technology
Faculty of Information Technology
Tallinn, Estonia

E-mail: maarik@taltech.ee; adrian.venables@taltech.ee; rain.ottis@taltech.ee

Abstract: *Preparation of cyberspace operations (COs) requires planners to consider technical peculiarities, which are not relevant in terms of planning traditional military operations (Barber, Bobo & Sturm 2015). Using Exercise Crossed Swords 2021 as an experimental test bed, a review of the latest NATO doctrinal developments, structured interviews, and a questionnaire were undertaken. The literature review revealed thirteen specificities of COs, and the interviews allowed for the identification of prerequisites for COs planning on strategic, operational, and tactical levels. The questionnaire highlighted four additional areas for improvement in CO planning. As a result of this investigation, twenty improvements to cyberspace operational planning are proposed.*

Keywords: *Cyberspace Operations Planning*

Introduction

Cyberspace is one of NATO's five operational domains. It was recognised as such in 2016 as the fourth domain joining land, sea, and air, and was followed by Space in 2019 (CCDCOE 2021). All NATO member states have national cybersecurity incident response teams, and many are still developing cyber operations capability to improve their capability in this domain. Additionally, NATO has agreed to set up a new Cyberspace Operations Centre as part of its strengthened Command Structure (CCDCOE 2021). There is also a growing interest in offensive cyber operations (OCO) for military purposes, which is expressed in the creation of NATO cyber commands, branches, or services within the armed forces (CCDCOE 2021). By 2022, 27 of the 30 NATO member states will have created cyber forces with Luxemburg, Montenegro, and North Macedonia remaining the exception. Training and exercising are conducted by the NATO-affiliated Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, which hosts the annual Exercise Crossed Swords (CCDCOE 2022). This exercise includes leadership training for the command element, legal aspects, and joint cyber-kinetic operations, in addition to the technical challenges (CCDCOE 2022). For the past two years, Estonia's Cyber Command Headquarters has been engaged in planning and executing cyberspace operations (CO) as part of a wider kinetic military operations process.

To assist commanders and their staff in operational planning, NATO has come out with several joint publications. These include the Allied Joint Doctrine for the Planning of Operations (NATO Standard AJP-5 2019) and the Allied Joint Doctrine for Cyberspace Operations (Ministry of Defence UK 2020). However, as planning for COs requires additional elements compared to what

is typically involved in kinetic military operations (Barber, Bobo & Sturm 2015), further planning methodologies should be identified. These include deeper technical planning on a tactical level.

This article identifies and critically analyses the key differences between planning land-based military operations and planning COs. These are categorized and assessed with recommendations for improving dynamic CO planning. The specific contribution of this work is to propose improvements in CO planning and execution. For this purpose, the key differences between them, which can be validated in subsequent cyber exercises, are identified.

Methods

This paper uses experimental research employing the design science methodology (Kosmol & Leyh 2019) with Exercise Crossed Swords as the platform for concept development, experimentation, and validation. Structured interviews were conducted to extract, document, and analyse information from subject matter experts focussing on established best practices, known challenges, and individual experiences.

To assess CO development, planning, and execution, a literature review was conducted to examine current developments and military doctrines. This compared the latest NATO military operational and CO doctrines with the Allied Joint Doctrines for the Planning of Operations, Cyberspace Operations, Joint Doctrine Note 1-8 Strategy, and Allied Joint Doctrine for the Joint Intelligence, Surveillance, and Reconnaissance. These detail the joint and multinational operation principles for kinetic and COs. Military operational planning is a sequence of activities undertaken by the commander and his or her staff at all levels (Ministry of Defence UK 2021). However, cyberspace has unique characteristics in that it is fabricated, partly nonphysical, and may not conform to geographical boundaries (Ministry of Defence UK 2020). Planning CO goes beyond what is typically required for kinetic military operations and these unique attributes require a different approach in their preparation and conduct (Barber, Bobo & Sturm 2015).

Following the literature review, structured interviews with the commander of the exercise CHQ were conducted, which were complemented by discussions with CHQ section commanders. This was supported by a questionnaire that was distributed to the cyber headquarters element (CHQ) members on the final day of the exercise using the Google Forms platform. From a total of 23 staff members, 19 completed the questionnaire.

Joint NATO doctrinal publications principles have been practised in Crossed Swords exercises since 2019. The staff element—their processes and structure—have evolved over this period to expose a research gap identifying the differences between kinetic and CO planning within NATO.

Results

This section presents the significant findings of the work, starting with the literature review, followed by the interviews, and concluding with the questionnaire results.

Results of the literature review

NATO has released many Joint Publications on CO and military planning. These publications are intended to assist member states in forming the basis for joint operational planning. The latest NATO Joint Publication for operations planning, AJP-5 The Allied Joint Doctrine for the Planning

of Operations, was published in May 2019 (NATO Standard AJP-5 2019). The most recent publication on COs, the Allied Joint Doctrine for Cyberspace Operations (Ministry of Defence UK 2020), was published in July 2020.

The review of the Allied Joint Doctrine for the Planning of Operations and the Allied Joint Doctrine for Cyberspace Operations resulted in the following key findings:

Rules of engagement

In CO and military operations, ROE is issued to the Commander based on his or her delegated authority. COs require an appreciation of a range of legislation, including international law, national law, the United Nations (UN) Charter, Law of Armed Conflict (LOAC), and human rights law.

Higher intent and plan

The CO commander's intent may include defensive or offensive operations. If offensive cyberspace operations (OCO) are planned, they will be conducted through the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism, by the principles agreed to by NATO (Goździewicz 2019). As NATO has not developed its OCO capabilities but relies on its Member States, the SCPEVA mechanism is used to request offensive cyber effects on a target (Goździewicz 2019).

Complete intelligence analysis of the adversary

Allied Joint Doctrine for Cyberspace Operations refers to Allied Joint Doctrine for Joint Intelligence, Surveillance, and Reconnaissance (NATO Standard AJP-2.7 2019). Cyberspace intelligence is based on availability and sharing. As NATO does not have its own organic cyber intelligence capability, it relies on allied nations to provide this service. This is seen in the Joint Intelligence, Surveillance, and Reconnaissance (JISR) system, where Allies collaborate to collect, analyse, and share information (Joint Intelligence, Surveillance, and Reconnaissance 2022).

Situational awareness of adversary forces

"Gaining situational awareness of adversary forces requires conducting significant intelligence collection, which requires the knowledge of the interconnectivity of networks" (Weiskopff 2017, pp. 22-3). Additionally, in the context of cyber targeting, it requires constant updating to validate intelligence and the positive identification of targets in near real-time (Weiskopff 2017).

Clear definition of cyber effects

CO effects may be categorised as either desired or undesired as well as direct and indirect effects. These are included but are not limited to secure, isolate, contain, neutralize, recover, manipulate, exfiltrate, degrade, disrupt, or destroy. The effects-based operations (EBO) system can be used for targets that are either tangible or abstract (Weiskopff 2017). No definition of EBO has yet been agreed on. Still, for this paper, EBOs are defined as the operations conceived and planned in a systems framework that considers the full range of direct, indirect, and cascading effects. These include the application of military, diplomatic, psychological, and economic instruments of power (Davis 2001).

NATO higher level support in expectation management

Traditionally, in military operations, expectation management is based solely on commanders'

guidance. In OCO the commanders' expectations are partly pre-determined by the SCEPVA mechanism because the NATO OCO capabilities depend on its Member States (Goździewicz 2019).

Dynamic cyber space environment analysis

NATO operations generally occur in a dynamic environment in which actors continually change the political, military, economic, social, infrastructure, and information (PMESII) elements (NATO Standard AJP-5 2019). In operations planning, the PMESII model may be supported or succeeded by JIPOE (Joint Intelligence Preparation of the Operating Environment). Additionally, the Joint Doctrine Note 1-18, Strategy (Joint Doctrine Note 1-18 Strategy 2018) uses the DIME (diplomatic, informational, military, and economic) model to describe national power instruments. This emphasises the complexity of dynamic cyberspace environment analysis.

Technical cyber intelligence gathering

In military operations planning, the commander, the operations planning group, and the more comprehensive staff must formulate their priority intelligence requirements (PIR) and Commander Critical Information Requirements Management (CCIRM) function. Based on these requirements, intelligence processes will be established, where operations branch staff and intelligence functions synchronize and integrate all collections capabilities to support operational planning. In CO, the planning staff identifies relevant aspects of cyber intelligence in coordination with the Cyberspace Operations Centre (CyOC) and other branches and capabilities throughout cyberspace layers—the physical, logical, and cyber-persona. The physical layer consists of hardware components, tied to geographic location, with the logical layer comprising software and data components. The cyber-persona layer does not consist of actual people or organisations but is rather an image of their virtual identity (Ministry of Defence 2020).

Wargaming

In military operations planning, the courses of action (COA) are evaluated with wargaming. In CO planning, the anticipated effects are included in assessing the COAs and would be validated with the Cyberspace Operations Centre (CyOC).

Detailed overview of own forces capabilities

In military operations planning, the operations planning group is advised to consult early with the subject matter experts (SME) of the respective functional areas within its staff and other commands and the respective doctrine. Risk management and vulnerability assessment are examples of activities that help to achieve a detailed overview of their own forces during the preparation of DCOs (Ministry of Defence 2020).

Multi-layered dimension

"Another difference between traditional warfare and cyber warfare is that traditional warfare exists exclusively in the physical world whereas cyber exists in both a physical world and a logical one" (Weiskopff 2017, p. 20). The Allied Joint Doctrine for Cyberspace Operations describes the logical layer as follows: "Entities at the logical layer are elements manifested in code or data, such as firmware, operating systems, protocols, applications, and other software and data components. The logical layer cannot function without the physical layer, and information flows through wired networks or the electromagnetic spectrum. The logical layer, along with the physical layer, allows

the cyber-persona to communicate and act". The recent NATO Allied Joint Doctrine for Cyberspace Operations recognises the persona layer as a separate dimension for conducting COs. The logical and persona layers are not necessarily linked to one specific physical location or device.

High availability of cyberinfrastructure

Conventional military operations, in general, have always been a mandate for state-sponsored entities. In contrast, the cyber infrastructure's vast interconnectivity and high availability provide a wide range of cyber criminals with almost the same opportunities to execute malicious actions in the cyber domain (Weiskopff 2017). Governments and states tend to use cyber criminals as mercenaries.

Targeting

Traditional targeting commonly refers to an exclusive geographical position. On the other hand, achieving the desired effect using cyber means requires considering targets' physical and logical targets at once (Weiskopff 2018). One logical target can be in multiple locations—for example, a virtual server/host.

The Results of the Questionnaire

Between 6-10 December 2021, the CCDCOE organized exercise Crossed Swords 2021 was conducted. A questionnaire was distributed among the cyber headquarters element (CHQ) to assess cyber operations development, planning, and execution. The questionnaire was conducted using the Google Forms platform on the last day of the exercise (9 December 2021). Of the total of twenty-three staff members, nineteen participated in the questionnaire. The results are presented per category of topics.

Cyberspace definitions

Cyber operations were described in nineteen different ways with no referral to known doctrines. Approximately 36% of respondents described cyber operations close to NATO AAP's 2020 cyberspace definition (NATO - AAP-06 2021). 73% of CHQ personnel did not understand cyber terms and concepts uniformly.

Staff tasking and training

The roles and responsibilities among CHQ posts need to be better defined. The Senior leadership required more experience and time to plan and execute cyber operations. 65% of the CHQ staff members self-assessed that their roles were not matched to their abilities. A little over one-third (35%) of the CHQ staff stated that it required more experience to fulfil its post tasks. A third of the answers suggested that experienced mentors were required, while 66% of answers suggested that there was a need to have more exercises.

Mission and awareness

It was identified that the mission of CHQ was not clear among CHQ staff. Less than half (47%) of the CHQ staff understands the operational environment.

Improving the planning of the exercise

To improve the CHQ Exercise structure, the following thirteen different changes were suggested:

1. Improve CHQ SOP (Standard Operating Procedure).
2. Add current ops positions.
3. Add plan ops position.
4. Add C35 (Communications Systems).
5. Add C5 (Cyber, Command, Control, Communications, and Computers Assessments).
6. Add a Cyber Situational Awareness cell.
7. Add info ops officer.
8. Add a targeting officer.
9. Add LNOs to components commands.
10. Add additional information manager.
11. Have more leadership.
12. One answer suggested having several CHQs or several teams in all sections for different outcomes and planning structures.
13. One answer suggested changing the CHQ structure to more like an actual staff structure, with roles and processes.

Over a third of the proposals suggested improving various parts of CHQ SOP. Legal advisors pointed out that they would want to be more involved in the planning of COs. Prior to conducting a major exercise, questionnaire responders confirmed that they would want to have more, smaller, connecting tabletop exercises. Another important issue has been related to CHQ staff, where just over half of them had the software tools necessary to fulfil their duties.

Results of the Interview

A structured interview was conducted after Exercise Crossed Swords 2021. The Interviewee was Uko Valtenberg (OF3-RES), Estonian Defence Forces Cyber Command, Cyber Operations Centre commander in reserve, and Commander of Exercise Crossed Swords 2021 Cyber Headquarters. The interview results presented prerequisites to plan CO at the CHQ level. The CHQ was intended to be an operational level HQ but also had tactical elements, and, overall, the CHQ structure was not clearly defined. The interview revealed that few structural roles, such as cyber intelligence, were not played or present. Secondly, the CHQ began its exercise during the operation's second phase, just before the attack was planned. Specific comments from the interview were categorized through strategic, operational, and tactical levels.

Strategic level prerequisites for planning a CO

It is imperative to have Rules of Engagement (RoE) and a mandate to operate in adversary territory. The CHQ must be provided with a higher commander intent and plan to ensure that operation goals align with joint operation objectives. Preliminary target propositions must be presented to the CHQ to narrow down the scope of planning. A complete intelligence-driven overview of the adversary must be established to allow the CHQ commander to make informed decisions. A full overview of their own forces (including Allies and neighbouring troops), restrictions, and a deconfliction matrix must be provided to the CHQ to ensure efficient coordination of different activities.

Operational level prerequisites for planning a CO

Situational awareness with regard to their own and enemy forces is critical from a CO planning perspective. Developed targets must be prioritized and categorized (for example logistics, energy, military, financial) by the higher-level HQ to support the planning and allocation of available

resources. Cyber effect principles must be clearly defined, understood (for example: degrade, disrupt, deny, destroy), and accepted by all units involved in the CO. In other words, the plan should follow the same principles as in cyber incident management. Cyber planning staff should have a fundamental understanding of information technologies, cybersecurity principles, and risk- and security assessment. Higher level commander support in expectation management is required to ensure technical capabilities correspond to the expectations of operation participants.

Tactical level prerequisites for planning a CO

A commander must have a detailed overview of his or her own force's technical capabilities. It is expected that operators have passed the following training:

1. General IT and cybersecurity training.
2. Individual specialized training.
3. Team exercises.
4. Mixed teams' exercises.
5. Harmonized maturity level assessment.
6. Internal team assessment.

Pre-prepared technical environment

Technical tools (such as non-traceable accounts in different services and systems) used during a CO must be prepared before execution of a CO. ICT infrastructure used for executing the CO must be obfuscated and distributed to impede attribution and efficient implementation of countermeasures by the adversary. "For red teams, using an obfuscated network for testing offers the advantage of hiding who is performing the attack and where it is originating, for a more real-life context. It lets the red team blend in with the normal network traffic while performing reconnaissance and test attacks in a more realistic manner" (Lawson 2021).

Tactical level units must have dedicated support resources with regards to maintenance of CO ICT infrastructure and relevant tools. This is required to speed up the CO by allowing operators to focus on the objectives, instead of conducting administrative tasks during CO execution.

Additional prerequisites for planning a CO

Political, Military, Economic, Social, Information, Infrastructure, and Physical Environment (PMESII) analysis of operational area must be conducted to enable adequate planning activities. Target-related technical cyber intelligence must be provided to the CHQ at every stage of the CO.

Discussion and Conclusions

The planning of cyber- and military operations entails differences at the strategic, operational, and tactical levels. The list of significant findings is presented below, prioritized by their importance:

1. The interview revealed that the preparation of the technical environment should be considered the key element for planning CO. Tactical commanders should prepare an obfuscated and distributed ICT infrastructure for both training purposes and for conducting actual COs. The primary purpose of obfuscating and distributing ICT infrastructure is to mask interrelations of its components, ensure operation continuity, and aggravate attribution if and when individual ICT components are revealed by the target. Creating

and utilizing the preprepared technical environment requires deep-technical planning. The details of the technical environment should be planned and implemented according to the objectives of COs. Additionally, preparation, implementation, and administration of the technical environment require that sufficient resources be allocated to ensure operational security (OPSEC) principles and operational objectives are met.

2. According to the literature review, the complete preparation of forces requires operation planners to consult SMEs during the initial stages of the planning process. Preparation of DCOs involves the execution of risk management and vulnerability assessment activities. However, preparing OCOs requires a deep understanding of their own units' capabilities to achieve mission effects.
3. According to the literature review, the CO planning staff should formulate technical cyber intelligence requirements at all layers of cyberspace: the physical, logical, and cyber-persona. Requirements must be synchronized and integrated with all collection capabilities. Cyber commanders and staff should formulate all the intelligence requirements, regardless of their nature, and submit them to supporting intelligence mechanisms.
4. According to the interview and literature review, the CO mission analysis should include the complete PMESII or more advanced methods (like JIPOE). The PMESII-PT analysis and other similar techniques, such as METT-TC (Haugli 2016) provide the cyber commander with even more value for planning and executing COs.
5. According to the interview and questionnaire, CO tactical level wargaming or Purple Teaming is required before a major exercise or operation. Although wargaming is not an everyday activity concerning COs, it should be considered a critical necessity with a special focus on the technical level. An isolated technical environment is the first requirement to conduct tactical level wargaming. Such a technical environment should be designed as a laboratory (O'Leary 2019) for conducting tests and experiments.
6. According to the literature review and interview, the list of cyber effects is not final, and effect parameters should consider the cyber incident management principles. The parameters of CO's effects should follow the cyber incident management principles. How much of the target is disrupted, 1%-100%? The same principles apply to integrity, availability, and confidentiality impact. An example of an effect requirement for a military tactical operation can be formulated as follows: degrade availability of target ABC 50%, starting from (date, time) to (date, time). "Effects-based operations apply to the cognitive domain, they have the ability to affect the decisions of political leaders, military commanders, or even whole populations" (Weiskopff, p. 40).
7. According to the literature review, targeting in COs must be executed at three layers: the cyber-persona, logical, and physical layers. The enemy should be considered a complex system during the execution of effects-based operations (Weiskopff 2017). This means that cyberspace is considered one of the different attack vectors that targeters can exploit to affect the target. Target development involves the systematic discovery of enemy system components, including the linkage of those components to the actual target and the possible effects on the target if specific components (or linkages) were manipulated. Targeting different components of the same system, through synchronized efforts of available capabilities and resources, can improve the efficiency of effects-based COs. Systematically and consistently planned and executed effects-based COs have the potential to create an impact on a national/state level (Weiskopff 2017). Additionally, it must be considered that, while targeting physical cyber-infrastructure, the destruction or disruption will have collateral damage. COs are conducted primarily on civilian ICT infrastructure, which will

have adverse effects on civilian ICT services.

8. According to the literature review, public cyber infrastructures can be used by cyber criminals to execute malicious actions in the cyber domain. The Sandworm Team, a division of the GRU (Russia's General Staff Main Intelligence Directorate), is an example of a threat group that is known to be using a given approach (MITRE ATT&CK 2017). Ukraine's energy facility was attacked by a Sandworm group in February 2022. Attackers succeeded in planting a new version of the Industroyer malware to disrupt ICS infrastructure at different levels (Brumfield 2022). The cyberattack was detected and prevented by the Ukrainian team. The Ukrainian activity can be considered a self-defence act. "Self-defence in international law refers to the inherent right of a State to use of force in response to an armed attack. Self-defence is one of the exceptions to the prohibition against the use of force under article 2(4) of the UN Charter and customary international law" (International Committee of the Red Cross 2022).
9. According to the literature review, the intelligence processes will be the same but will rely on various sources. NATO does not have its own organic cyber intelligence capability and relies on allied nations to provide this service. A cyber commander should establish and maintain Cyber Intelligence Sharing procedures and channels with allies, partnering intelligence services and cyber incident response communities.
10. According to the literature review, it must consider a set of military doctrines to achieve complete intelligence concerning an adversary. The AJP3.20 doctrine is meant for addressing CO-specific planning. But still, it is related to two dozen other principles. The cyber commander should not focus solely on the cyber doctrines but must orient it in the maze of allied principles
11. According to the questionnaire, CO definitions are not uniformly understood. COs are an emerging discipline, whereas conventional military operations are better understood. It is recommended to use the latest cyberspace definitions for joint COs and exercises published by NATO.
12. According to the questionnaire and interview, the cyber-capable planning staff is a crucial necessity for planning CO. The commanders are responsible for training and preparing the team and for achieving the necessary cyber capabilities. Cyber planning staff should have a fundamental knowledge of information technology as well as a broad understanding of cybersecurity and the risks involved.
13. According to the questionnaire and interview, the CO planning staff should have a harmonized maturity level. The planning staff performs its tasks more unanimously and efficiently if its expertise levels are the same or close to each other.
14. According to the questionnaire, significant enhancements should be implemented to improve situational awareness of the cyber-operational environment. Two significant steps should be taken towards improvements in the operational situational awareness. First is to follow the "CRR Supplemental Resource Guide, Volume 10: Situational Awareness" (Carnegie Mellon University 2016). Secondly, it is necessary to plan and implement a visual tool for presenting and synchronising operational (situational awareness) information from different operation levels.
15. According to the questionnaire, the structure of CO in the headquarters element (CHQ) needs to be revised. It is not clear what the structure of a cyber-HQ staff should be. The proposed structure improvements should be implemented, evaluated, and validated in the following exercises.
16. According to the questionnaire, planning and executing COs require more specific tools.

Cyber commanders should be aware that the development and testing of custom software elements is a time-consuming process. Therefore, the requirements and functionalities must be carefully defined and budgeted promptly. The results of software development activities must eventually help to improve the following:

a. Internal and external cooperation.
b. Situational awareness of the operational environment.
c. Analysis of technical cyber-intelligence.
d. Task- and data-flow management.

17. According to the questionnaire and interview, the CO staff needs to pass a variety of additional training, along with individual specialized training, team exercises, mixed teams exercises, and internal team assessments. The planning staff needs to develop a coherent training plan to achieve a synchronised maturity level. The staff must be trained regularly, until it is capable of planning and executing CO as a team.
18. According to the questionnaire and literature review, legal advisors should be more actively involved in the operation planning process. Operation planners must consider the complex legal environment and involve legal advisors in every step of the operation.
19. According to the literature review, CO relies on cyber intelligence sharing, so liaisons should be involved in relevant branches and capabilities. The CO commander should appoint liaisons to partner branches and ensure appropriate channels and tools are used for (cyber-technical) intelligence sharing. An example of an open-source cyber threat-sharing tool is the MISP (MISP 2022).
20. According to the literature review, OCO involves coordination with the SCEPVA mechanism. NATO does not develop its OCO capabilities but relies on its Member States. The SCPEVA mechanism is used to request offensive cyber effects on a target. This means that cyber-capable nations may be asked to deliver offensive cyber effects on a target assigned by an operational-level commander (Goździewicz 2019).

These findings form the basis of CO planning improvements and should be considered in future CO doctrines, processes, and methods. The significance of this work is to clarify and improve the future of the planning and execution of CO. CO research is limited to exercises, as real-life operations are nationally classified. Subsequent cyber exercises should validate the findings of the current work.

As the usage of digitally assisted weapon systems during modern kinetic military operations inevitably increases, the importance of CO will raise exponentially. Command and control systems, communication networks, GPS-guided missiles, and pre-warning systems (like air-, sea- and land radars) are likely to become high-priority cyberspace targets.

Acknowledgements

The writer would like to express special gratitude to his colleagues at Talgen Cybersecurity OÜ: Mr Uko Valtenberg and Mr Kim Vahturov. Their cyberoperations-related experience allowed for valuable discussions and contributed to the quality of this publication.

References

Barber, D, Bobo, A & Sturm, K 2015, 'Cyberspace operations planning: Operating a technical military force beyond the kinetic domains', *Military Cyber Affairs,* vol. 1, no. 1, pp. 1-8, viewed 19 March 2022, <https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1003&context=mca

/>.
Brumfield, C 2022, 'Ukraine energy facility hit by two waves of cyberattacks from Russia's Sandworm group', viewed 6 November 2022, <https://www.csoonline.com/article/3656954/ukraine-energy-facility-hit-by-two-waves-of-cyberattacks-by-russia-s-sandworm-group.html>.

Carnegie Mellon University 2016, 'CRR supplemental resource guide,' vol. 10, *Situational Awareness*, Version 1.1, viewed 5 November 2022, <https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-SA_0.pdf>.

Cooperative Cyber Defence Centre of Excellence (CCDCOE) 2021, 'Cyber defence', 2 July, viewed 19 March 2022, <https://www.nato.int/cps/en/natohq/topics_78170.htm/>.

—2022, 'Crossed Swords', viewed 19 March 2022, <https://ccdcoe.org/exercises/crossed-swords/>.

Davis, PK 2001, 'Effects-based operations a grand challenge for the analytical community', viewed 23 May 2022, <https://www.rand.org/content/dam/rand/pubs/monograph_reports/2006/MR1477.pdf>.

Goździewicz 2019, 'Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA), viewed 10 May 2022 < https://www.cyberdefensemagazine.com/sovereign-cyber/>.

Haugli 2016, 'METT-TC – What does it actually entail?', viewed 10 May 2022, <https://primaryandsecondary.com/mett-tc-what-does-it-actually-entail/ />.

International Committee of the Red Cross, 'Self-defence', viewed 6 November 2022, <https://casebook.icrc.org/glossary/self-defence#:~:text=Self%2Ddefense%20in%20inter national %20law,Charter%20and%20customary%20international%20law>.

Joint Doctrine Note 1-18 'Strategy' 2018, viewed 18 May 2022, <https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_18.pdf/>.

Joint Intelligence 'Surveillance and Reconnaissance' 2022, viewed 3 May 2022, <https://www.nato.int/cps/en/natohq/topics_111830.htm#:~:text=NATO%20has%20established%20a%20permanent,Alliance's%20deterrence%20and%20defence%20posture.>.

Kosmol, L & Leyh, C 2019, 'ICT usage in industrial symbiosis: Problem identification and study design', *Annals of Computer Science and Information Systems*, vol 18, pp. 685-92, viewed 19 March 2022, <https://annals-csis.org/proceedings/2019/drp/pdf/323.pdf>.

Lawson, G 2021, 'Securityweek 2021, How to improve red team effectiveness using obfuscation', 18 November, viewed 16 April 2022, <https://www.securityweek.com/how-improve-red-team-effectiveness-using-obfuscation>.

Ministry of Defence (UK) 2020, 'Allied Joint Publication (AJP-3.20): Allied joint doctrine for cyberspace operations', viewed 19 March 2022, <https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320/>.

—2021, 'Allied Joint Publication (AJP)-5(A) Allied Joint Doctrine for the planning of operations', updated March 2021, viewed 19 March 2022, <https://www.gov.uk/government/publications/allied-joint-publication-ajp-05a-allied-joint-doctrine-for-the-planning-of-operations/>.

NATO Standard AJP-5 2019, 'Allied Joint Doctrine for the planning of operations', viewed 19 March 2022, <https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_144557/story_content/external_files/AJP-5_EDA_V2_E.pdf />.

NATO Standard AJP-2.7 2019, 'Allied Joint Doctrine for the joint intelligence, surveillance and reconnaissance', viewed 19 March 2022, <https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP27.pdf>.

NATO - AAP-06 2021, 'STANAG 3680 - NATO glossary of terms and definitions (English and French) - AAP-6', viewed 19 March 2022, <https://standards.globalspec.com/std/14486494/aap-06>.

MISP Threat Sharing, viewed 12 May 2022, <https://www.misp-project.org/download/ />.

MITRE ATT&CK 2017, 'Sandworm Team', viewed 11 June 2022, <https://attack.mitre.org/groups/G0034/>.

O'Leary, M 2019, *Cyber Operations: Building, Defending, and Attacking Modern Computer Networks*, APRESS, Towson, MD, US.

Weiskopff, M 2017, 'Effects-based operations in the cyber domain`, viewed 23 May 2022, <https://apps.dtic.mil/sti/citations/AD1033006 >.

Appendix 2

Publication II
Arik, Marko; Venables, Adrian; Ottis, Rain (2024). The Optimal Organisational Structure for Cyber Operations based on exercise lessons. ECCWS 2024: 23rd European Conference on Cyber Warfare and Security.

The Optimal Organisational Structure for Cyber Operations based on Exercise Lessons

Marko Arik, Adrian Nicholas Venables and Rain Ottis
Department of Software Science, Tallinn University of Technology Tallinn, Estonia.

marko.arik@taltech.ee
adrian.venables@taltech.ee
rain.ottis@taltech.ee

Abstract: The NATO Cooperative Cyber Defence Centre (CCDCOE) of Excellence hosts annual Locked Shields (LS) and Crossed Swords (CS) cyber exercises to help NATO nations develop, train, and test their cyber capabilities. These exercises have successfully experimented with cyber capabilities and human organisational structures. However, there are still opportunities to optimise cyber exercise structures. This article employs a use case study based on these exercises to compare structures used by NATO nations in cyber exercises and cyber operations. This identified an optimal structure for operational-level cyber defence and offence exercises and proposed methods for their planning, development, and execution.

Keywords: Cyber Operations Exercises, Cyber Command organisational structure, Blue Team organisational structure, Red Team organisational Structure.

1. Introduction

Cyberspace threat actors can exploit advanced nations' reliance on the information environment, necessitating the establishment, training, and preparation of a military force to counter adversary activities. However, countries developing cyber defence capabilities are often reluctant to disclose specific information about them. Cyber exercises can contribute to the e training and preparation of cyberspace forces and the development of their operational-level organisational structures. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) organises two well-known annual cyber exercises, Locked Shields[1] and Crossed Swords[2], to assist nations in developing, training, and testing their cyber capabilities. This research examines the cyber capabilities and structures by collecting and interpreting new data to analyse the Operational and Tactical levels of Command. This addresses the challenge of obtaining reliable data from non-classified exercises to reveal cyber organisations' optimum Command structures.

2. Methods

This article employs a use case study based on the 2022 Locked Shields and Crossed Swords cyber exercises organised by the CCDCOE. It provides an overview of NATO Cyber Operations and exercise organisational structures. The literature review examined the Locked Shields exercise from “after-action” reports used for research purposes. Interviews with experts from Estonian Defence Forces Cyber Command, CCDCOE, Locked Shields 2022 Red Team, and NATO Cyberspace Operations Centre supplement the review.

3. Literature Review

Three sources were used for data in this research. As the leading global cyber power, the US offers insight into large organisations' structures (Voo et. al., 2022, p. 11). The smaller Estonian Cyber Command and its organisational structures were also reviewed as the exercises were organised by the CCDCOE based in Tallinn, and data on its composition was available. Finally, the publicly available NATO Cyber Operations (CO) command organisational structures are reviewed (Pederson et al., 2022), (Dalmijn et al., 2020), (Blumbergs, 2019), (Kohler, 2020).

3.1 Cyber Operation Organisational Structures

In the Routledge Handbook of International Cybersecurity, Piret Pernik states the role of a cyber command as follows:

[1] https://ccdcoe.org/exercises/locked-shields/
[2] https://ccdcoe.org/exercises/crossed-swords/

"At a minimum, a cyber command should be composed of staff sections (capabilities) for strategic and policy analyses and planning (including legal and technological development), intelligence, situational awareness, operational planning, and conduct of cyber operations. A military centre of excellence for research and competence and a cyber range should support the cyber command. Finally, the command should have a degree of authority for the acquisition and personnel policies (including reserve forces and conscription if applicable), as well as education, training, and exercises" (Pernik, 2020). In addition, the organisation's success depends on its members' training and experience to succeed (Pomerleau, 2022)

An article by Air Land Sea Space Application Center (Pederson et al., 2022) discusses cyber operations structures. The current USCYBERCOM cyberspace operations structure is a temporary fix, a 'band-aid' that patches the infrastructure using the least expensive materials. For the optimal solution, Pedersen proposed a separate standing organisational structure as the optimal solution for U.S. military forces and the protection of DOD cyberspace from adversaries (Ibid). The subsequent structures include more details concerning the organisations' roles and departments or teams.

2020, the CCDCOE published 'The Cyber Commanders` Handbook' (Dalmijn et al., 2020). This stated, "A one-size-fits-all Cyber Command structure is impossible to define." Instead, the handbook proposed a reference organisational structure, which includes the core activities of cyber operations. The Cyber Commanders' Handbook outlines an organisational structure with four levels: Commander, Advisors, Staff, and Subcommand. Specialised branches facilitate military cyber operations, including C2 for situational awareness, C3 for cyber defence, C5 for planning, and C6 for communications. Legad provides legal guidance on national and international laws in cyber operations.

A different cyber operations structure focused on Specialized Cyber Red Team Responsive Computer Network Operations was proposed by Blumbergs (Blumbergs, 2019). Dr. Blumberg's concept of Red Team (RT) can be expanded to offensive cyber operations in general. It is not restricted to narrow "red teaming" or opposing force framework but is a product of the CCDCOE exercise culture where Blue Teams are on the defence, while the Red Teams are on the offensive role. This was done in a very abstract version of the chain of command. This described the chain of command based on the specific activity focus area, shown in white in Figure 1.

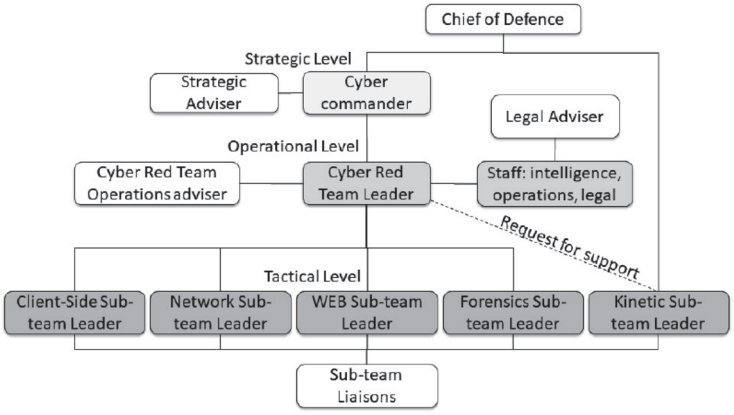

Figure 1: Exercise Crossed Swords 2019 Cyber Red Team chain-of-command (Blumbergs, 2019).

The 2019 Crossed Swords exercise adapted this structure to introduce a chain-of-command model with grey rectangles representing the Cyber Red Team at political, strategic, and tactical levels. Chain-of-command represents a hierarchy of authority in which each position is accountable to the one directly superior. This highlighted linkages to exercise control functions and sub-teams are based on expertise in targeted technologies.

An alternative model is utilised in Estonia's Defence Forces Command organisational structure by Kohler (Kohler, 2020). This offers an example of how the organisational structure of the Cyber Command can be located inside the broader Armed Force's organisation.

The Cyber Commanders' handbooks provide a helpful reference organisational structure for those nations seeking to establish an initial capability. In addition, Dr Blumberg provides a basis for developing Cyber Red

Teaming structures for exercises. These structures for peacetime cyber operations should be independent of other military Services and supported by research and cyber range capabilities.

3.2 Selected Cyber Exercises Organisational Structures Review

The Locked Shields 2022 Blue Teams' "after-action" reports reveal their organizational structures, with 14 out of 23 reports providing an overview. Multi-nation structures were excluded because they are often operation/case-specific and thus temporary. This research resulted in reviewing nine national team structures, including the related functional components such as the departments or teams within the organisation. An analysis of these structures focused on identifying commonalities and differences. Figure 2 illustrates the organisational structure of each team. The horizontal axis represents the team number, and the vertical axis represents the elements in the organisation. The minimum number was eight elements, the maximum was 23, and the average team consisted of 14 elements. The elements of the structures represent the roles and departments or teams within the organisation.

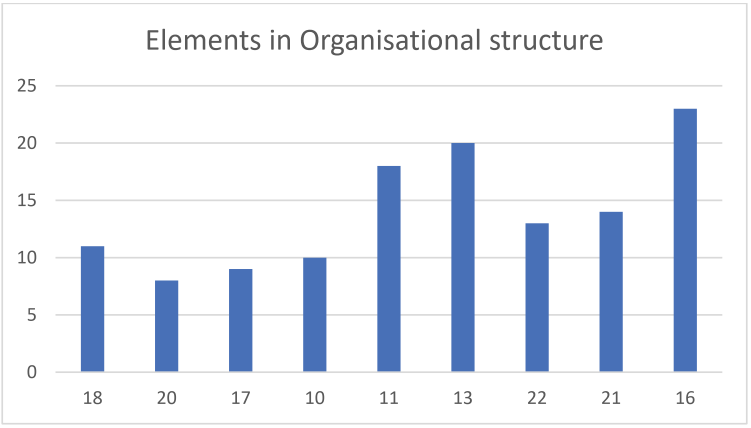

Figure 2: Exercise Locked Shields 22 selected Team Elements in Organisational Structure.

Figure 3 illustrates the number of personnel in each team. The average was 80 persons per team, with the smallest number being 50 and the largest comprising 102 people. The horizontal axis represents the team number against the number of personnel in each team.

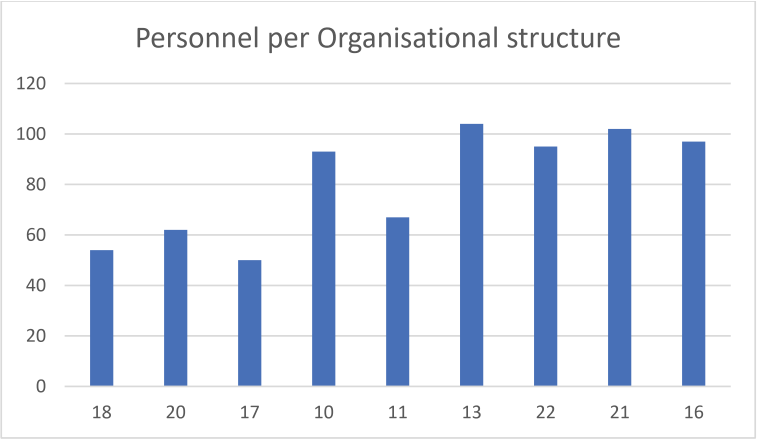

Figure 3: Exercise Locked Shields 22 selected Team Personnel per Organisational structure.

Error! Reference source not found. indicates the proportion of each team with earlier experience in a similar exercise.

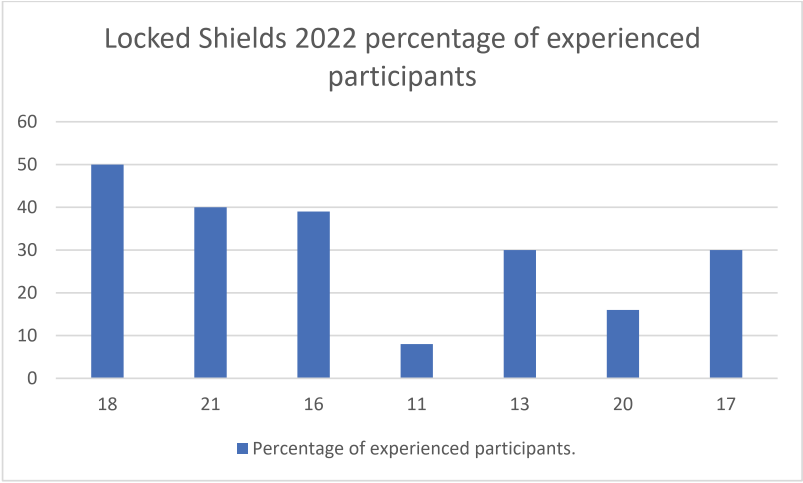

Figure 4: Locked Shields 2022 percentage of experienced participants.

The following section highlights the key attributes of a sample of a team's organisational structure.

The organisational structure of team Number 18 is shown in Figure 5. It should be noted that this team was the winner of the exercise. The winning score was calculated by CCDCOE's exercise evaluation team and is based on a complex scoring algorithm, which includes factors such as cyber-attacks successfully defended, availability of defended assets, forensics and legal.

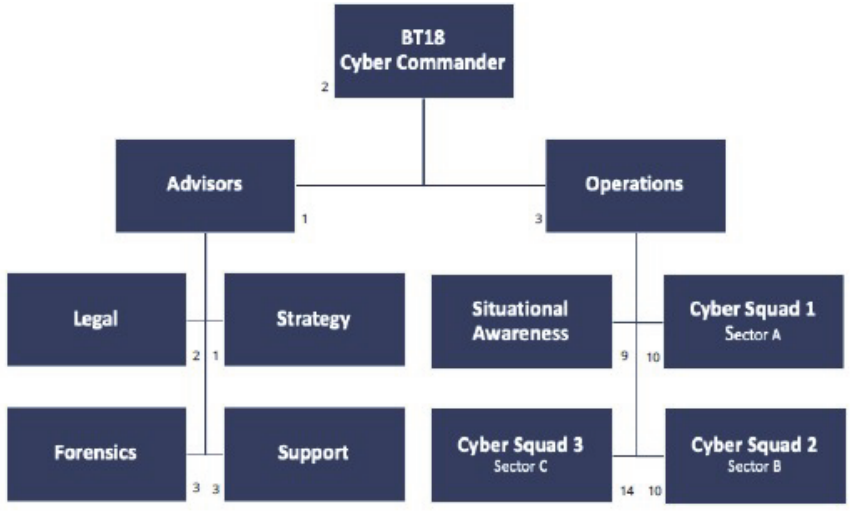

Figure 5: Exercise Locked Shields 2022 Blue Team 18 organisational structure.

Team number 20 had an operational framework and objectives based on various software applications. A little over a quarter of the team had participated in previous similar exercises. Based on the exercise scoring system, the team's results were in the last third.

Team number 17 had team objectives in place, and their strategy and tactics were derived from their national Standard Operational Procedures (SOP). Many tools were used, both in-house and externally provided. The team was placed close to last based on the exercise scoring system.

Team number 10 utilised a capability-based approach, focusing on results unrelated to team size. Capability-based planning is an approach that ensures that changes in an organisation are aligned with the overarching strategic vision. Their unique organisational structure includes a Task Group, Tactical Operations Commanders, and a Joint Cyber element. The team's results were in the bottom third.

Team number 11, organisational structures, used elements from different domestic organisations. These elements originated from the nation's military, governmental and academic sectors. Based on the exercise scoring system, the results of this team were slightly below average.

Team number 13 comprised 104 participants from 25 organisations with a complex organisational structure. Based on the exercise scoring system, the team's results were in the last third. However, they planned to maintain this structure for subsequent exercises, with only a proposed increase in information-sharing and reporting aspects.

Team 22 combined military and civilian personnel with six sub-elements and was placed in the top five.

Team 21 comprised 102 participants from 25 organisations, including private companies, energy, finance, national police, military, and telecoms. Despite providing their team objectives, the strategy and tools used were withheld from the report. This team was placed in the top ten.

Team number 16 had 97 participants from private and governmental sectors, including the military, public agencies, and academia. A distinctive feature of this team was the inclusion of a Finance element, and they were also placed in the top ten.

The results of the "after-action" reports are summarised in Table 1, and their similarities are highlighted.

Table 1: Exercise Locked Shields 2022 AAR summary.

Strategy in place	Tactics in place	Goal set	Tools	Previous LS experience	Military leader	Forensics el. in structure	Legal el. in structure
66%	44.00%	88.00%	88.00%	75%	77%	55%	88%

4. Results of the Interviews

While preparing for the Crossed Swords exercise, an interview was held with the cyber headquarters' chief of staff (COS) (CHQ). The CHQ was the only operational-level headquarters involved in the exercise. The interview was focused on the organisational command structure for the exercise.

The command element organisational structure is shown in **Error! Reference source not found.**6 and was based on the previous year's exercise. Based on the exercise feedback, mentors were added for the 2022 exercise organisational structure. The exercise feedback was received through the questionnaire that the article's author conducted in December 2021. These were utilised to share knowledge and pass the experience to the new cyber operators (Gaston, 2022).

In 2022, CHQ initially utilised the Military Decision-Making Process (MDMP) to develop Standard Operating Procedures. However, the lead author of this paper proposed an alternative approach called Intelligence Preparation of the Cyber Environment (IPCE) (Lemay et al., 2014) to complement the MDMP process. The military decision-making process (MDMP) is an iterative planning methodology. However, the IPSE complements it with a detailed intelligence planning process to address the limitations of cyber operations planning.

The CHQ aimed to create an operational plan for sub-units, practice MDMP, and improve procedures. They focused on planning tasks, aligning tasks with relevant kinetic military units, and considering interactions between the Air Force, Navy, and cyber units. The Commander had complete command of the tactical units, divided into Defensive (DCO) and Offensive (OCO) teams. Live exercise units are marked in **Error! Reference source not found.** 6 with dotted lines.

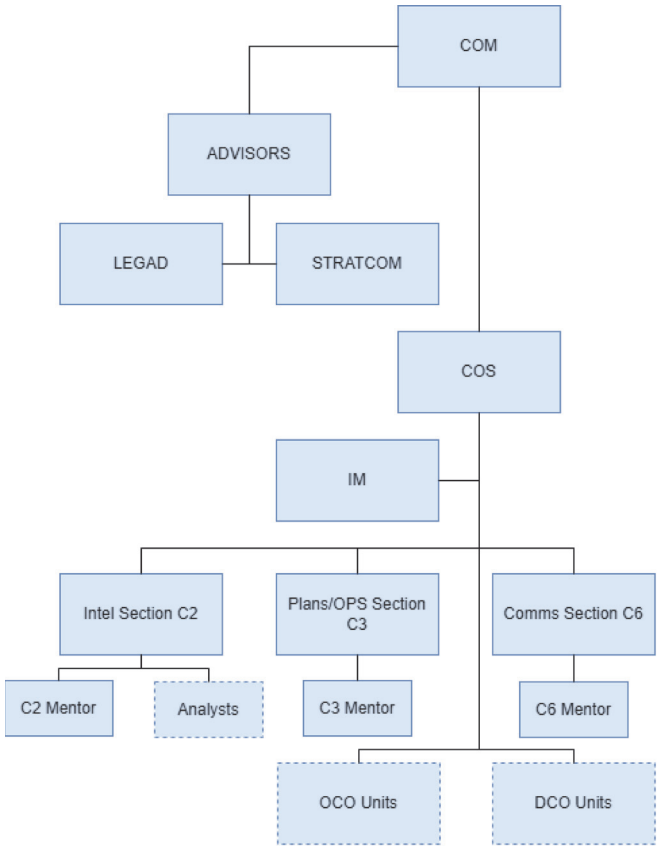

Figure 6: Estonian Defence Forces Cyber Exercises 2022 CHQ organisational structure.

The challenge in creating a cyber exercise command structure is appointing suitably qualified and experienced staff to critical positions. These include technical operators and intelligence and operations personnel to ensure a clear and comprehensible structure for military entities. The exact number of C2 and C3 positions should be proportional to the intensity of the exercise. The most critical roles from the CHQ planning perspective are C2, C3, COS, and Legad.

4.1 LS 2022 Case Study

In April 2022, the CCDCOE held the international cyber defence exercise, LS 2022, which involved 2000 participants from 32 nations (Papp, 2022). At the beginning of the exercise, the Red Team leader was interviewed to determine the prerequisites for conducting Red Teaming.

Successful Red Teaming exercises in tactical units require a two-day workshop, rigorous screening, and subjective assessment. Emphasising the importance of harmonised teams, the Red Team leader assembles sub-teams and identifies non-harmonized teams as a known weakness leading to mission failure. Novel aspects include recognising the significance of understanding Blue Team's motivations, the ability to develop custom tools, and adaptability to exercise the infrastructure's tempo. These prerequisites ensure a robust foundation for effective Red Teaming operations, encompassing technical readiness, strategic understanding, tool development proficiency, and flexibility in response to exercise dynamics.

The second interview with the Red Team leader took place in September 2022. The interview was about preparing an organisational command structure for Locked Shields. The interview aimed to illustrate and specify the details of the Read Team organisational command structure.

The Red Team's management methodology is based on twelve years of experience in cyber exercises. This allows the Red Team leader to plan and control activities without a detailed order, utilising good memory, common sense, and realism. The Red team composition is shown in *Figure* 7.

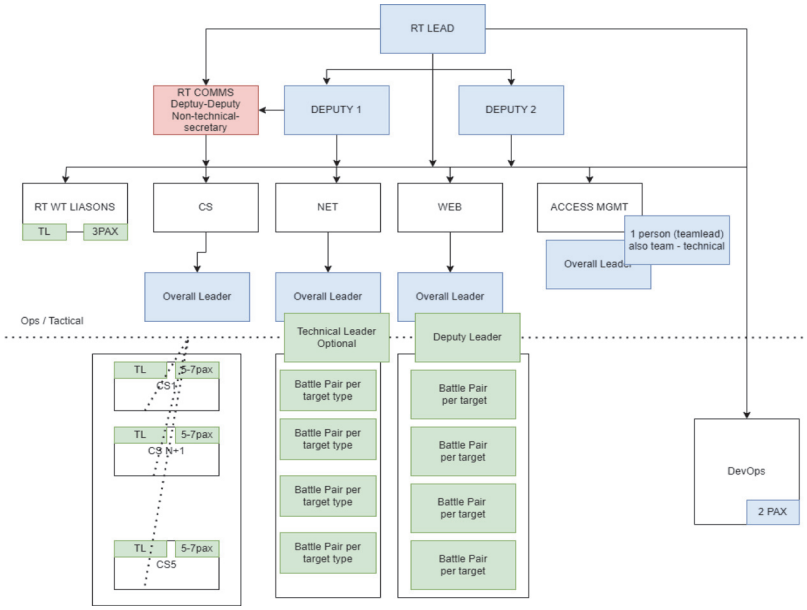

Figure 7: Exercise Locked Shields 2022 Red Team organisational structure.

The Red Team structure during the Locked Shields exercise consists of the following sub-teams: network (NET), client-side (CS), web application (WEB), and access management team. The NET team handles network attacks, the CS team prepares and executes client-side attacks, and the WEB team handles web application attacks.

The Red Team leader and their two deputies managed the major DevOps and COMMS teams. These created technical tools for the Red Team and managed information and human resources. The CS team had five sub-teams led by a Team leader, with five to seven subordinates, compared to NET and WEB teams, which were divided into battle pairs per target type.

The Red Team leader created a scalable structure depending on the size of the exercise, with the operational level handling mission planning and the tactical level engaging targets. The technical team leads with field experience supporting operational planning, while other participants support the command element. Sub-teams are involved with CS, NET, and WEB mission development to execute decisions during planning.

A further interview was conducted with a former military officer who has experience planning cyber operations. The interview highlighted the differences between real-life and exercise structures and was conducted before the CS 2022 execution period in November 2022.

The interview suggested that a headquarters' organisation is determined by exercise objectives and the Commander's experience or can be created through dialogue between higher command and tactical units. It was highlighted that a rule of thumb in military structures is that a commander should have at most seven subordinates to ensure the effectiveness of command and control (C2) activities. The meaning of command is the authority delegated to someone/somebody to give orders and directions, and control – is the ability to influence the execution of the orders mentioned above by allocating or withholding resources needed. This applies to cyber organisations as well as conventional military structures.

4.1.1 Locked Shields

LS exercises follow procedures to maintain the technical integrity of the network, which can prevent operational testing due to planning constraints. However, real-life operations have no restrictions, with politicians deciding priorities.

Blue Teams are often pre-formed with internal C2 structures and pre-agreed procedures created for mutual understanding and interoperability. However, this setup has limitations, requiring minimal modifications and preventing operational-level involvement.

4.1.2 Crossed Swords

In contrast to LS, most of the CS training audience (TA) is brought together as individuals only for the exercise execution without prior collaboration training. The structures formed for the exercise cannot go through team dynamics such as forming, storming, norming, and performing. This describes the path teams follow to high performance (Tuckman, 1965).

The CS exercise enables cyber headquarters personnel to simulate real-world scenarios, training in a realistic and dynamic environment. In contrast, the LS exercise maintains fixed rules, limiting its focus to technical aspects and revealing operational gaps due to shorter planning times. Participants need help integrating technical, operational, and strategic layers, particularly in the operational domain, where resources may need to be increased. Preparing competent cyberspace officers, establishing specific goals, and considering Joint Multinational Training Center (JMRC, 2022) courses are recommended to address this. Drawing inspiration from a similar training approach at the Joint Multinational Training Center in Germany, incorporating full-time military unit engagements against opposing forces could be a valuable future enhancement for CS exercises.

The CS Cyber Command element headquarters (CHQ) for the observed exercise was established Ad hoc. It was compiled from individual experts rather than involving an established vertical organisational structure. This provided the opportunity for CHQ to utilise previously developed and tested SOPs. The exercise provides an opportunity to test and re-assess the SOP and implement improvements based on the experience gained. In 2022, CHQ planned to develop and test its SOP. An iterative planning methodology known as the military decision-making process (MDMP) was used to comprehend the situation and mission, devise an action plan, and create an operating plan or order. The MDMP is designed against a predictable enemy who follows a doctrinal approach.

Based on the US Marine Corps Cyberspace Training and Readiness Manual, the recommendation is to create a Mission Essential Task List (METL) to address operational issues (NAVMC, 2018). The METL aids in defining organisational structures, tools, and equipment for planning, developing, and executing cyber operations. An example of Mission Essential Task List Relations in the Crossed Swords Exercises is provided in Figure 8.

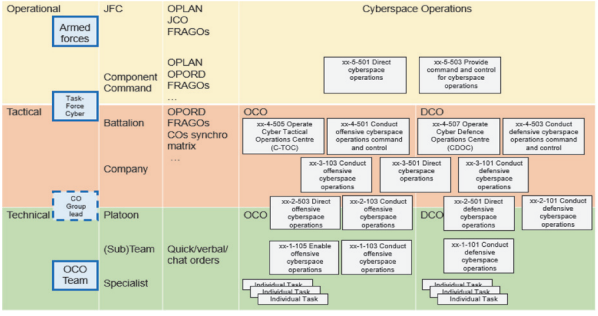

Figure 8: Example Mission Essential Task List Relations in the Crossed Swords Exercises.

A concluding interview transpired with a Plans Staff Officer within the NATO Cyberspace Operations Centre (CYOC). It was asserted that the exercise's command and control (C2) framework ought to be meticulously delineated, encompassing due consideration for the headquarters' inherent processes and procedures. The structural configuration should be tailored to align with the distinct objectives of the training audience, contingent upon their hierarchical positioning within the organisational framework.

Regarding the differences between cyberattack and -defence organisational structures, NATO's official policy is defined as "NATO is a defensive alliance with no plans to develop its offensive cyber capabilities. In cyberspace, as in all other domains, NATO acts in line with its defensive mandate and international law" (Ackerman, 2019). Therefore, it can be concluded that NATO has not developed its own OCO capabilities. Instead, it relies on its Member States. The Sovereign Cyber Effects Provided Voluntarily by Allies (SCPEVA) mechanism requests offensive cyber effects on a target (Goździewicz, 2019).

An exercise organisational structure requires a clear understanding of roles, responsibilities, and authority, addressing all functional areas without overlapping responsibilities. Integrating cyberspace into all HQ functions is the best practice. Different exercises should focus on training technical, operational, strategic, and political participants. A diverse range of stakeholders is crucial for success. Additionally, innovative aspects of the layered exercise design are proposed. Recommending distinct exercises for technical, operational, strategic, and political level participants to address their specific training requirements.

4.2 Findings from the Interviews

The main challenge in building a cyber exercise command structure is staffing the required positions, selecting people with the appropriate cyberspace competencies, and having well-instructed sub-team leaders. A goal-oriented structure with seven to eight subordinates is essential, with technical leads providing opinions on operational planning. Cyber operations exercises should involve strategic and operational planning, including cyberspace experts and trusted agents. Addressing the operational level planning resource gap is crucial, with a proposed Joint Multinational Training Center as a potential solution. To excel, create a cyberspace-specific framework for planning and execution, set training objectives, and effectively manage time. The uniqueness of a cyber exercise command structure lies in its specialised staffing, technical focus, goal-oriented approach, inclusion of cyberspace experts, international collaboration, cyberspace-specific framework, and emphasis on addressing operational challenges specific to the cyber domain. A Mission Essential Task List (METL) is crucial for organisational structures, setting mission-critical tasks with necessary tools and equipment. This study proposes Intelligence Preparation of the Cyber Environment (IPCE) as a supplement to the iterative MDMP, providing a detailed intelligence planning process to enhance cyber operations planning.

5. Results

An analysis of the organisational structures of the Blue Teams participating in LS enables structural elements to be correlated with the place achieved in the exercise. Figure 9 shows that in the top three teams (teams nr 18, 22, and 21), the number of elements in their organisational structure ranges from eleven to fourteen. Although this might suggest that the most optimal number of organisational elements is in this range, further research is required to analyse each team's skill set. No clear indication of an optimal team size based upon this limited sample size is recognised, and these results represent only Exercise Locked Shields 2022.

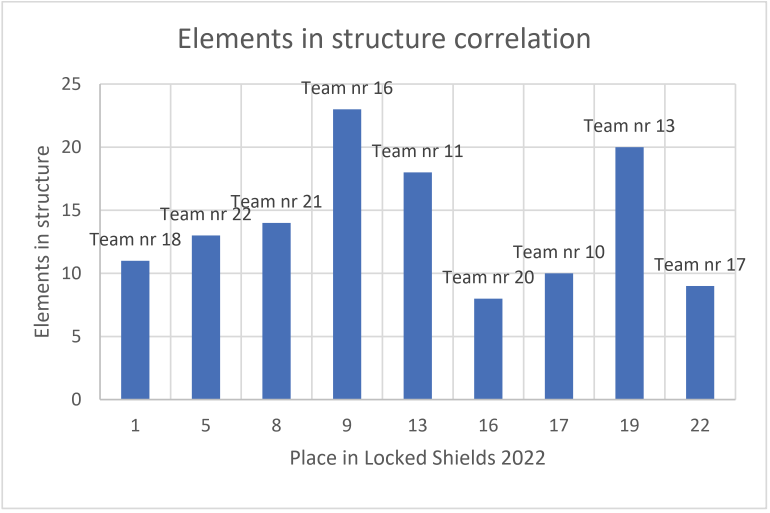

Figure 9: Exercise Locked Shields selected Blue Teams organisational structure, element count correlation.

A further characteristic recognised is the number of people per organisational structure. This is illustrated in Figure 3 and Figure 10, which illustrate the personnel appointed in each team's organisational structure in correlation with the place achieved in the exercise. The top three teams are highlighted on the left side of the graph. Their personnel count per organisational structure remains between 54 and 102. The personnel to organisational structure element ratio for the first-place team is 4.9, for the second 7.3 and the third 7.2. The

22nd team had a ratio of 5,5, and the 19th-place team had a ratio of 5.2. This indicates that the ratio of the number of people per organisational structure and the team size is irrelevant to the team's overall success. Over half of the observed teams had more than 80 persons per organisational structure. This might indicate that the number of people per organisational unit and units per team does not significantly influence the team's success.

Figure 10: Exercise Locked Shields selected Blue Teams organisational structure, personnel count correlation.

The study analysed team composition and personnel count per organisational structure. The winning team had 11 elements, 54 personnel, and an average 4.9 personnel-to-structure element ratio. The correlation between place in the exercise and number of people was -0.09, suggesting a need for more relevance in success. The study reveals that success in the Locked Shields exercise relies on well-defined strategies, clear training objectives, technical readiness, and personnel experience, with team size and structural elements not determining success.

Successful teams in the Locked Shields exercise have standard skill sets, including military commanders, forensics, and legal advisors. They prioritise strategic planning and collaboration, engaging organisational structure members 3-4 months before exercise execution. They rely on customised software tools, demonstrating adaptability and commitment to technology readiness.

The success of LS team structures relied on effective leadership, specialised elements, early planning, and tailored software tools, providing valuable insights for cybersecurity exercise preparedness.

In compiling all the data collected, the optimal structure for the Locked Shields Blue Teams may consist of 11 elements and 55 personnel. At a minimum, there must be the following elements: a commander, Legad, forensics, and technology capabilities. Based on the exercise's technical challenges, up to eight separate Technology Capabilities elements might be included. These skillsets are shown in Figure 11 and could include capabilities such as Industrial control system (ICS), Network, Windows, Linux, Monitoring, Web, Mobile and Threat Hunting.

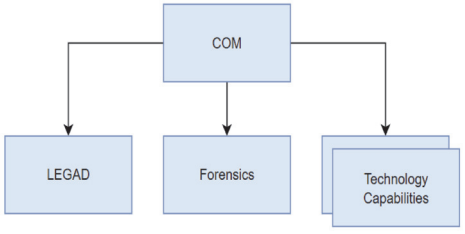

Figure 11: The Optimal Blue Team Structure for Locked Shields Exercise

6. Conclusions

The research emphasises the need for adaptive organisational structures in cyber exercises, addressing challenges unique to cyber operations training. A resource gap in cyber headquarters development requires preparing competent officers and leveraging training programs. This underscores the complexity of cyber exercises, emphasising continuous improvement and flexibility in structures and training to meet incipient expectations.

Cyber power countries are adjusting their cyber operations structures for future employment, requiring modifications to their Cyber Commanders Handbook and goal-specific structure for NATO exercises.

The Estonian Defence Forces Command's organisational structure is an example, and nations should consider the need to train dedicated cyber ranges. Dr. Blumbergs' designed chain-of-command for the Crossed Swords exercise is advantageous, as it outlines the hierarchy of tactical, operational, and strategic levels.

The top three Blue Teams' organisational structure elements in Exercise Locked Shields 2022 were 11-14, with 8-15 elements, although there needed to be a clear correlation and further analysis is required. As for conventional exercises, cyber exercises should include tactics, strategies, objectives, and tools with experienced individuals. Military commanders are preferred to the team, with members forming 3-4 months before an exercise. The Blue Teams structure typically includes Legal, Strategy, Advisors, and Operations, which are managed by the headquarters Plans/Operations (C3) sections. The EDF Cyber Exercises 2022 CHQ structure faced challenges in filling the necessary planning staff, as cyber operations planners' competencies are uncharted, requiring further research. The structure should be proportional to the exercise level and complexity.

Dr. Blumberg's design of the Red Team's organisational structure for Locked Shields is nearing optimal. With team leaders having no more than five to seven subordinates, goal-oriented is supported by interviews and provides an optimal and scalable structure for Red Teaming exercises.

A distinctive feature of the Red Team is that no specific direction is needed depending on the attackable systems and experience of the Red Teamers. However, Blue Teams need a higher command level to plan and maintain DCO. Therefore, planners and commanders must understand this essential difference and that roles, procedures, and tools differ. Red Teams focus on recruiting individuals with practical and hands-on skills relevant to cyber operations. In contrast, blue teams manage structures that categorise members based on specific skill sets, such as specialising in cybersecurity products or defendable assets. The need for additional research is emphasised, suggesting that further investigation or exploration is required to understand and refine the distinctions and roles within these teams. Red Teamers require special tools, infrastructure, and planning time, with good sub-team leaders and harmonised teams.

Planning officers must understand command-and-control authority and chain-of-command differences and integrate cyber into all HQ functions to prepare for entire spectrum operations, integrating kinetic and cyber operations.

Exercise participants face technical, operational, and strategic challenges, particularly at the operational layer. Cyber headquarters structural evolution needs faster development, with increasing numbers of competent officers and specialists needed. CHQs need to improve SOP and cyber operations planning, using alternative methods and setting goals during execution. However, in-depth planning is challenging due to strategic, operational, and tactical differences between cyber and other operations.

The research recommends implementing the US Marine Corps Cyberspace Training and Readiness Manual's recommendation for creating a Mission Essential Task List to enhance preparedness and operational response.

As cyber exercises increase in complexity, the command-and-control aspect for each headquarters becomes more critical. The CYOC experience underscores the need for diverse technical, operational, strategic, and political layers in one exercise, fostering trust and building cyber operations training structures.

This research revealed the complexity of cyber exercises and the importance of planning, training, and collaboration to address the unique challenges of cyber operations. It also highlights the need for adaptation and flexibility in organisational structures to meet the evolving demands of cyber operations training.

References

Ackerman. (2019) “NATO Cyber Policy Under Construction”, [online], https://tinyurl.com/txwufe8b
Blumbergs. (2019) “Specialized Cyber Red Team Responsive”. Tallinn: Tallinn University of Technology.
Dalmijn et al. (2020) Cyber Commanders’ Handbook. In NATO CCDCOE Publications (pp. 26-27). Tallinn: North Atlantic Treaty Organization.
Gaston. (2022) “Air Force officers share paths to personal and professional success with cadets”, [online], https://tinyurl.com/bdwhyd3a
Goździewicz. (2019) “Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA)”, [online], https://tinyurl.com/4zjydnpe
JMRC. (2022) “7th Army Training Command. Retrieved from 7th Army Training Command”, [online], https://www.7atc.army.mil//
Kohler. (2020) “Cyberdefense Report: Estonia’s National Cybersecurity and Cyberdefense Posture. Zürich: ETH Zürich”.
Lemay et al. (2014) “Intelligence Preparation of the Cyber Environment (IPCE)”, Journal of Information Warfare, Vol. 13, No. 3 (2014), pp. 46-56.
NAVMC. (2018). NAVMC 3500.124. Department of the Navy Headquarters United States Marine Corps.
Papp. (2022) “Locked Shields 2022 - Multinational Cyber Defense Exercise”, [online], https://defence.hu/news/locked-shields-2022-multinational-cyber-defense-exercise.html
Pederson et al. (2022) “DOD Cyberspace: Establishing a Shared Understanding and How to Protect It”, [online], https://tinyurl.com/y6dvyn4p
Pernik. (2020). Handbook of International Cybersecurity. Routledge: National Cyber Commands.
Pomerleau. (2022) “DoD must focus on skilled cyber defenders, not just new tech, warns weapons tester”, [online], https://tinyurl.com/4fzyu6c2
Tuckman. (1965) “Developmental Sequence in Small groups”, [online], https://tinyurl.com/2xymzt7z
Voo et al. (2022) “National Cyber Power Index 2020”, [online], https://tinyurl.com/2aukkv4z

Appendix 3

Publication III

Arik, Marko; Lugo, Gregorio, Ricardo; Ottis, Rain; Venables, Adrian (2024). Competencies Required for the Offensive Cyber Operations Planners. HCI International 2024, 26th International Conference on Human-Computer Interaction.

Competencies Required for the Offensive Cyber Operations Planners

Marko Arik(✉), Ricardo Gregorio Lugo, Rain Ottis, and Adrian Nicholas Venables

Tallinn University of Technology, Tallinn, Estonia
marko.arik@taltech.ee

Abstract. This paper presents a systematic review of competencies required for Offensive Cyber Operations planners. Military Cyber Headquarters staff must possess strategic, operational, and tactical skills for effective planning and execution of cyber operations at different levels. This article examines the necessary skills for Offensive Cyber Operations (OCO) planners at the operational level. The research aims to define the role of an operational-level OCO planner, identify necessary skills, and develop a framework for practical OCO planning, requiring further research and development. This systematic review utilises academic databases and includes peer-reviewed studies on Offensive Cyber Operations planning competencies, encompassing journal articles, books, and conference papers.

Keywords: Cyberspace operations planning · Cyberspace planners' competencies · Cyberspace · Cyber operation officer · Offensive Cyber Operations · CO decision maker · Systematic ReviewFirst Section

1 Introduction

Mapping the abilities and competencies required for a military's Cyber Headquarters staff members is vital to the organisation's success (Joint Publication 1 2013). Cyber Operations (CO) planners must have military planning experience and an in-depth knowledge of cyberspace operations (United States Army War College 2022, p. 32). When assembling a cyber team, knowing which skills and experience are required is crucial to fulfilling each assigned position's goals. Cyber Operations are handled at three levels: strategic, operational, and tactical, and the skills involved at each differ (AJP-3.20 2020) The strategic level needs a greater understanding of political goals and situational understanding. Operational-level planning requires using cognitive skills from commanders and their staff, and at the tactical level, technical skills are needed.

The article focuses on the operational level, which is essential because the operations' design and management are conducted at this level (NATO Standardization Office 2020, p. 19). The military doctrine also refers to it as' operational art' and involves (Joint Pub 5–0 1995) planning operations and effects to achieve strategic objectives. This article explores the required competencies for Offensive Cyber Operations (OCO)

A. Moallem (Ed.): HCII 2024, LNCS 14729, pp. 20–39, 2024.
https://doi.org/10.1007/978-3-031-61382-1_2

planners at the operational level. Understanding the factors contributing to cyber operators' performance is imperative to improve education and training for military personnel (Jøsok et. al. 2019). In addition, recent research reveals a need to organise offensive cyberspace operations and their impact (Huskaj and Axelsson 2023). However, certain obstacles include a lack of suitably qualified personnel with the requisite skills (Ibid). Previous research regarding cyber operations has mostly focused on DCO (Defensive Cyber Operations) and, more specifically, at the tactical level of cyber operators (Jøsok et. al. 2019).

This research applies a detailed examination and academic rigour to identify the necessary competencies required for OCO planners. Specifically, the goals of the study are:

1. To define the role of an operational-level OCO planner.
2. To identify the operational skills, digital skills, soft skills, and experience required for the competencies needed at the operational level of an OCO planner.
3. To devise a framework (including a training plan, skillset, and all required competencies) to become a competent OCO planner.

The three goals commence with a fundamental understanding of the issues. Our final stage will inform applied research aspects, highlighting the requirements for further research and development to incorporate civilian and military education, training modes and framework development.

Several NATO countries have acknowledged that OCO planning has become more mainstream. For example, the 2016 NATO Warsaw Summit addressed the OCO capabilities in the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism. NATO's current policy is that it "does not go offensive in cyberspace" and that the Alliance[1] does not create organic offensive cyber capabilities. Therefore, it must consult with its Member States to deploy offensive capabilities, and the SCEPVA mechanism is currently used. Nations with cyber capabilities may be asked to launch offensive cyber effects against a target chosen by an operational-level commander (Goździewicz 2019). The SCEPVA construct enables the integration of offensive cyberspace operations capabilities in operations despite challenges in coordination. Although not the most effective way to utilise allies' combined OCO potential, it provides a pragmatic framework for NATO training (Jensen 2022). SCEPVA allows NATO member nations to contribute cyber capabilities to NATO missions while maintaining command and control over them. Due to the increasing significance of cyber operations in collective defence and deterrence, it is essential to understand how deploying cyber capabilities may influence conflict dynamics (Libicki and Tkacheva 2020, p. 61). Control over SCEPVA remains with the contributing nation, and offensive cyberspace operations during Alliance missions require approval. Planning staff assess cyberspace, considering potential effects while acknowledging that integrating force elements may not always be feasible. Additionally, there is a need for continuous interaction and updates due to the evolving nature of cyberspace (AJP-3.20 2020, pp. 23,27). The SCEPVA mechanism is the critical driver

[1] Alliance / allies refers to North Atlantic Treaty Organization.

of OCO's capabilities while providing an opportunity for operations. The RSA Conference 2016 keynote also advocated a proactive approach against hackers through Information Operations, including Active Defence and Offensive Countermeasures (ENISA 2016). These measures aim to gather intelligence and counteract adversaries. However, ethical and legal considerations, along with challenges in attribution, pose significant risks. An EU legislative framework needs to be more consistent across member states. While Information Operations offer advantages, carefully considering legal, technical, and ethical implications is crucial (Ibid). Based on the preceding, this article focuses on operation-level military aspects and offensive cyberspace training frameworks.

2 Methods

Using PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) for literature reviews in offensive cyber operations offers significant bene-fits. PRISMA provides a systematic and transparent approach, enhancing replication (Tricco et al. 2018; Moher et al. 2015). It helps identify key findings and ensures quality in research selection, which is crucial in the varied quality of cyber operations sources. PRISMA reduces bias through a predefined selection process and criteria.

PRISMA's systematic framework is widely used for defining research questions and criteria for including and excluding studies. It allows for a thorough literature review, identifying gaps and guiding future research (Moher et al. 2015; Tricco et al. 2018). This is particularly relevant in the rapidly evolving field of cyber operations.

Our study involved academic sources like journals, books, reports, and theses, focusing on offensive cyber operations planning skills. We included 13 studies, selecting scholarly documents and excluding those not related to offensive cyber operations competencies and duplicates.

2.1 Review Procedure

1. Identify literature on Offensive Cyber Operations planners' competencies through database searches.
2. Sort the publications into categories based on type.
3. Provide a summary of the identified papers in order of research questions.
4. Synthesis, discussion of the findings, and recommendations for further study.

2.2 Literature Collection Methodology

The years of publishing ranged from 1990 to 2023, with only English-language articles reviewed. Table 1 includes a list of databases and search phrases.

Table 1. Overview of databases, search terms, hits and last search date.

Database	Terms searched	Hits	Last search date
GoogleScholar	"offensive cyber operations planners competencies", "offensive cyber operations competencies", "cyber operations competencies", "cyberspace operations planner", "cyber offensive planner", "cyber operations planner", "cyberspace planners competencies", "cyber planners competencies", "cyber operational planner"	16	26.09.2023
ScienceDirect	"offensive cyber operations planners competencies", "offensive cyber operations competencies", "cyber operations competencies", "cyberspace operations planner", "cyber offensive planner", "cyber operations planner", "cyberspace planners competencies", "cyber planners competencies", "cyber operational planner"	0	26.09.2023
IEEE	"offensive cyber operations planners competencies", "offensive cyber operations competencies", "cyber operations competencies", "cyberspace operations planner", "cyber offensive planner", "cyber operations planner", "cyberspace planners competencies", "cyber planners competencies", "cyber operational planner"	0	26.09.2023
DuckDuckGo	"offensive cyber operations planners competencies", "offensive cyber operations competencies", "cyber operations competencies", "cyberspace operations planner", "cyber offensive planner", "cyber operations planner", "cyberspace planners competencies", "cyber planners competencies", "cyber operational planner"	7	26.09.2023
Taylor& Francis	"offensive cyber operations planners competencies", "offensive cyber operations competencies", "cyber operations competencies", "cyberspace operations planner", "cyber offensive planner", "cyber operations planner", "cyberspace planners competencies", "cyber planners competencies", "cyber operational planner"	0	28.09.2023

3 Results

To Define the Role of an Operational-Level OCO Planner. The Google Scholar database provided 16 returns to the search terms. Of these, there were 13 suitable studies. DuckDuckGo database provided an additional seven results. Of these, there were two suitable studies. Eight studies were excluded due to not directly including any significance on OCO planners' definitions or competencies. Table 2 overviews the publications discovered and categorises them by type and methodology. Since no quantitative publications were identified, Table 2 represents qualitative and mixed (qualitative and quantitative) publications.

Table 2. Overviews the publications discovered and categorises them by type and methodology.

Subject	Basic information		Type	Methodology	
	Author(s)	Year		Qualitative	Mixed
Integrating Cyber with Air Power in the Second Century of the Royal Air Force	Withers et al	2018	Journal Article	X	
Cyberspace Operations Planning: Operating a Technical Military Force beyond the Kinetic Domains	Barber et al	2016	Journal Article	X	
The Cyberspace Operations Planner	Bender, J	2013	Journal Article	X	
A Cognitive Skills Research Framework for Complex Operational Environments	Neville et al	2020	Technical Report	X	
Joint Targeting in Cyberspace	Smart	2011	Report	X	
Let Slip the Dogs of (Cyber) War: Progressing Towards a Warfighting U.S. Cyber Command	Mulford	2013	Report	X	
Educating for Evolving Operational Domains	RAND Corporation	2022	Research Report	X	
A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0)	Shoemaker et al	2016	Book		X
The Cyberhero and the Cybercriminal	Nizich	2023	Book		X

(*continued*)

Table 2. (*continued*)

Subject	Basic information		Type	Methodology	
	Author(s)	Year		Qualitative	Mixed
Knowledge Management Application to Cyber Protection Team Defense Operations	Curnutt et al	2021	Master Thesis	X	
Thriving Cybersecurity Professionals: Building a Resilient Workforce and Psychological Safety in the Federal Government	Houston	2019	Master Thesis		X
Incorporating Perishability and Obsolescence into Cyberweapon Scheduling	Lidestri	2022	Master Thesis	X	
Implications of Service Cyberspace Component Commands for Army Cyberspace Operations	Caton	2019	Monograph	X	

The Cyberhero and the Cybercriminal (Nizich 2023) have used the NICE (The NICE Workforce Framework for Cybersecurity[2]) to define the Cybersecurity roles. For example, the Cyber Operations Planner develops detailed plans for conducting or supporting the applicable range of cyber operations through collaboration with other planners, operators, and analysts. They participate in targeting selection, validation, and synchronisation and enable integration during the execution of cyber actions. Knowledge Management Application to Cyber Protection Team (CPT) Defence Operations (Curnutt and Sikes 2021) defines a Cyber Planner. These perform vital functions throughout the assessment process involving coordination with CPT leadership /higher headquarters elements, tracking and planning Future Operations, and supporting Current Operations to activated Mission Element teams. Those filling the Cyber Planner role are typically experienced in two or more Cyber Mission Force work roles across defensive and offensive mission sets. This paper also proposes future research for Offensive Cyber Teams.

[2] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center.

Table 3. Navy Cyber Operation Planners Skills and Abilities.

Skills	Abilities
Critical Thinking	Written Expression
Judgment and Decision Making	Deductive Reasoning
Complex Problem Solving	Originality
Coordination	Inductive Reasoning
Systems Analysis	Problem Sensitivity
Writing	Information Ordering
Systems Evaluation	Communication
Active Learning	Written Comprehension
Monitoring	Fluency of Ideas
Quality Control Analysis	Selective Attention

This article also defined a CO planner: "Cyber operations planners help develop and coordinate analyses to perform defensive or offensive missions" (Houston 2019, p. 8).

The following is an example of defining the Cyber Operations Planner, although this is a governmental contract. "The Cyber Operations Planner is responsible for monitoring and reviewing strategies, doctrine, policies, and directives for compliance in cyberspace operations, providing input for briefings, transitioning concepts, and developing tactics and procedures" (U.S. General Services Administration 2022).

Identify the Operational Skills, Digital Skills, Soft Skills, and Experience Required for the Competencies Needed in the Operational-Level OCO Planner. Competencies are the knowledge, skills, abilities, and behaviours contributing to individual and organisational performance (National Institute of Health 2023). The Cognitive Skills Research Framework compares cyber operations competencies, focusing on cognitive tasks in cyber-attack and defence (Neville et al. 2020). This framework can identify skills and training needs for cyber attackers and defenders. It also examines competencies in cyber intelligence analysis and targeting, an essential skill for Offensive Cyber Operations (OCO) planners (National Institute for Standards and Technology framework).

Research emphasises the importance of targeting in cyberspace operations (Nizich, 2023; Bender 2013; Barber et al. 2016). While targeting is a known skill among military personnel, specific proficiencies in OCO and Defensive Cyber Operations (DCO) are less common (Smart 2011). Effective targeting in cyberspace requires understanding the law of war, the cyber centre of gravity, and operational planning. Cyber operations also need an understanding of cyberweapon perishability and obsolescence (Lidestri 2022).

Additionally, OCO planners must understand network metadata analysis and integrate cyber operations into broader command plans (Mulford 2013). The National Initiative for Cybersecurity Careers and Studies (NICCS) outlines specific competencies and training for cyber ops planners at various levels. Other sources, like Caton (2019),

suggest competencies in professional networking and information systems technology for cyber planners.

The NICE Cybersecurity Workforce Framework (2.0) defines competencies in counterespionage and operational security for cyber operations (Shoemaker et al. 2016, p. 36). RAND Corporation (2022) highlights the importance of civilian and military education in developing OCO planner competencies. Cyber operations require a deep understanding of the domain and integrated planning skills (Withers et al. 2018). Effective cyber planners also need comprehensive training programs, as Bender (2013) suggested, which proposes various courses for practical OCO planning.

Finally, the Navy Personnel Command (2023) details the role of Cyber Operation Planners, emphasising analytical support, targeting selection, and executing cyber actions. This illustrates the broad range of competencies required for effective OCO planning (Table 3).

The results section highlights the diverse knowledge, skills, abilities, and experiences needed for individuals in various roles related to cyber operations planning, including Offensive Cyber Operations (OCO) planners. This underlines the importance of ongoing education, training, and self-development to build competencies in this dynamic and critical field. Tables 4 and 5 present knowledge, skills, and abilities identified from the literature review, while Table 6 presents abilities.

Table 4. Knowledge identified from the literature review.

	Knowledge
1	Understanding of Cyberspace Operations, strategies, doctrine, policies and directives
2	Knowledge of tactics, techniques, procedures, concept of operations, and course of action development
3	Knowledge of current and emerging Cyber Threats
4	Understanding of perishability and obsolescence factors related to Cyberweapons
5	Knowledge related to Cyberspace Operations, including doctrine, policies and directives
6	Knowledge of cyberspace core competencies and cybersecurity activities
7	Knowledge of professional networking, social collaboration, and cross-functional data sharing
8	Understanding cyberspace, including threats, vulnerabilities, and intelligence collection capabilities
9	Knowledge of joint functions and operational procedures
10	Knowledge of kill chain framework and cyber threat analysis

A Proposed Framework Required for an OCO Planner. Bendler& Felderer's (Bendler and Felderer 2023) examination of the current landscape of competency models in the information security and cybersecurity fields analysed 27 existing models through qualitative content analysis, identifying a predominant focus on professional competencies while noting a significant underrepresentation of social human aspects,

Table 5. Skills identified from the literature review.

	Skills
1	Cognitive skills related to cyber operations include intelligence analysis and targeting
2	To analyse network metadata
3	To develop detailed plans for the conduct of cyber operations
4	To conduct battle damage assessments
5	To target analysis, including considerations of attribution and the principle of self-defence in cyberspace
6	To plan and coordinate Future Operations and Current Operations support
7	Analytical skills for supporting the planning process
8	Cognitive skills in cyber intelligence analysis, advanced cyber warfare, and network operations
9	Skills in information security, troubleshooting, information systems, and risk management
10	Technical planning skills and operational procedures
11	Planning and coordination skills in areas like targeting selection and synchronisation
12	Skills in analysing the kill chain framework for cyber threats
13	Proficiency in enterprise information systems technology
14	Skills related to data analysis and logistics
15	In Critical Thinking
16	In Judgment and Decision Making
17	In Complex Problem Solving
18	In Coordination
19	In Systems Analysis
20	In Writing
21	In Systems Evaluation
22	In Active Learning
23	In Monitoring
24	In Quality Control Analysis

and methodological competencies. Addressing these gaps, Bendler and Felderer propose that competency models must encompass a broader spectrum of skills and attributes necessary for cybersecurity professionals and should be comprehensive and able to bridge the divide between educational outputs and labour market requirements. Such models should have a continuous evolution and adaptation that can adjust to the rapidly changing cybersecurity landscape but must consider holistic approaches that integrate technical and non-technical competencies.

The above literature review shows the breadth of domain knowledge and skills needed for OCO personnel. Previous research (Chowdhury and Gkioulos 2021) found

Table 6. Abilities identified from the literature review.

	Abilities
1	Ability to coordinate with CPT leadership, higher headquarters elements, and Mission Element teams
2	The innate potential to perform mental and physical actions or tasks related to cyber operations planning
3	Abilities related to professional networking, social collaboration, and cross-functional data sharing
4	Abilities in core cyber-specific functions
5	An intuitive understanding of the cyberspace domain and potential capabilities
6	Ability to lead joint operations and develop cyber capability, doctrine, and tactics
7	Ability to conduct OCO effectively
8	Abilities for ongoing intelligence gathering and planning to deter or defeat cyber-attacks
9	The ability to develop and coordinate analyses for defensive or offensive missions
10	In Written Expression
11	In Deductive Reasoning
12	In Originality
13	In Inductive Reasoning
14	In Problem Sensitivity
15	In Information Ordering
16	In Communication
17	In Written Comprehension
18	In Fluency of Ideas
19	In Selective Attention

that cybersecurity competencies and skills can be broadly categorised into four main groups:

1. Technical Skills include the specific, hands-on abilities required to operate and protect cybersecurity systems. Technical skills are foundational for any cybersecurity role and typically involve knowledge of computer networks, systems administration, an understanding of cybersecurity tools and software, and the ability to detect and respond to cyber threats and vulnerabilities.
2. Managerial Skills: Managerial skills in cybersecurity pertain to the ability to oversee cybersecurity teams, projects, and initiatives. This involves strategic planning, resource allocation, risk management, and policy development. Managerial skills are crucial for ensuring that cybersecurity practices align with the organisation's broader objectives and that resources are effectively utilised.

3. Implementation Skills: Implementation skills refer to the practical application of cybersecurity strategies and policies. This involves deploying security measures, managing cybersecurity operations, and ensuring compliance with relevant standards and regulations. These skills are critical for translating cybersecurity strategies into practical actions that protect critical infrastructures.
4. Soft Skills: Soft skills are increasingly recognised as essential in cybersecurity. These include communication skills, problem-solving abilities, teamwork, and adaptability. Soft skills are crucial for effective collaboration, clear communication of technical information to non-technical stakeholders, and adapting to the constantly evolving landscape of cybersecurity threats and technologies.

While these Findings are Not Specifically for OCO Planners, Many Aspects are Similar. This section presents the training plan, knowledge, skills, abilities and experience to become a proficient OCO planner. The framework is devised from the literature review results and the NICCS Cyber Ops Planners' knowledge, skills, and abilities. The final list of OCO planners' knowledge, skills, abilities, and training plans is presented in Dataset 1, "The Framework for Offensive Cyber Operations Planners[3].

3.1 Training Plan

The proposed courses to become a practical OCO planner are detailed below. It should be taken into account that the names of the courses may have changed over time, and an equivalent course should be identified. The proposed OCO planner's training plan is presented in Table 7.

These courses prepare students for planning full-spectrum cyberspace operations, including attack, intelligence, surveillance, target acquisition, reconnaissance, defence, and environmental preparation. The courses are designed for U.S.-only students and provide an operator's perspective on network exploitation and vulnerabilities. Candidates must be U.S. citizens. The courses cover military doctrine, cyber threats, and electromagnetic spectrum fundamentals. Most of these courses are aimed at U.S. citizens and those serving in the Army. European equivalent courses can be found in the NATO CCDCOE training catalogue (NATO CCDCOE 2023).

The NICCS proposed Capability Indicators for Cyber Operational Planners, which include a range of topics divided into two proficiency levels. At the Entry level, individuals receive training in areas such as joint cyber analysis, joint advanced cyber warfare, and cyber network operations.

The training covers a broader spectrum of topics for Intermediate and Advanced levels. The recommendation for intermediate-level education is a bachelor's degree, while for advanced-level education, a master's degree is recommended. While these degrees are beneficial, they are not mandatory, and individuals from diverse educational backgrounds, practical experience, and certifications can pursue successful cyber operations planning careers. This includes advanced cyber warfare, network attacks, cyber operations, information security, troubleshooting, information systems, business processes, risk management, SQL, and Unix. This training is designed to provide a comprehensive

[3] https://drive.google.com/file/d/1OvtqROjVtrFIzW_mJ2Lr4mUzf7X98s10/view?usp=sharing.

Table 7. Proposed OCO planner's training plan.

Course name	Description	Knowledge Areas
National Defence University "CAPSTONE" course	Explains joint warfighting concept, security environment, conflict dynamics, operational and strategic levels. Emphasises Allied and Partner contributions	Joint warfighting, security environment, conflict dynamics, operational and strategic levels, Allied and Partner contributions
Information Operations Command's Basic CNO Planners Course	Utilises case studies and scenarios for planning criteria, effects, capability choice, success/failure, collateral effects, and battle damage assessments. Based on joint doctrine and U.S. DoD tactics	Joint warfighting, security environment, conflict dynamics, operational and strategic levels, Allied and Partner contributions
Army Cyberspace Operations Planners Course	Prepares for planning full-spectrum cyberspace operations, including attack, ISR, defence, and integration into Army and Joint planning processes. U.S.-only students	Full-spectrum cyberspace operations, attack, ISR, defence, and integration into planning processes
Cyber 200/300	Provides operator's perspective on network exploitation and vulnerabilities, integrating into the joint fight against cyber threats for U.S. Armed Forces	Network exploitation, vulnerabilities, and joint fight against cyber threats
Cryptologic Network Warfare Specialist qualification course	Focuses on advanced capabilities in cyberspace operations, cryptology, electronic warfare, signals intelligence, and space. U.S. citizens only	Cyberspace operations, cryptology, electronic warfare, signals intelligence, space
Joint Network Attack Course (Cyber Capabilities Developer Officer Course)	Provides initial training in military doctrine, cyber threats, cyberspace and electromagnetic warfare operations, and electromagnetic spectrum fundamentals. U.S. citizenship is required	Military doctrine, cyber threats, electromagnetic warfare operations, spectrum fundamentals

(*continued*)

Table 7. (*continued*)

Course name	Description	Knowledge Areas
Joint Advanced Cyberspace Warfare Course	Covers full-spectrum cyberspace operations, global cryptologic platforms, intelligence community, threats, planning, and analysis. Exclusive for U.S. Cyber Command	Full-spectrum cyberspace operations, global cryptologic platforms, intelligence community, threats, planning, and analysis
Joint Information Operations Planners Course	Focuses on planning, integrating, and synchronising full-spectrum information operations into joint operational-level plans. Open to multinational students	Information operations planning, integration, synchronisation, military deception, operations security, interagency coordination, and intelligence preparation
Joint Intermediate Target Development Course	Teaches research and documentation for developing virtual targets. U.S. Joint Chiefs of Staff course	Researching, documentation, virtual target development

skill set for cyber planners, allowing them to effectively plan and execute cyber operations while ensuring information security, troubleshooting, and aligning strategies with business processes and risk management considerations.

These courses are recommended by different authors and organisations based on their structured content. The courses cover various aspects essential for effective cyber operations planning in a military context. At the same time, providing comprehensive coverage of cyber warfare, joint military planning, information operations, and technical knowledge is critical for OCO planners.

3.2 Knowledge

The literature review contributes to NICCS Cyber Ops Planners' knowledge set by providing a more focused and specific set of knowledge and skills directly relevant to the role of an operational-level OCO planner. While the NICCS Cyber Ops Planners knowledge set offers a comprehensive list of knowledge, skills, abilities, and experience related to cybersecurity and network operations, literature review results narrow these requirements to those specifically needed for planning and executing offensive cyber operations.

The results help to define and specify the competencies required for individuals in the role of an OCO planner. It complements the more general knowledge areas listed in the NICCS Cyber Ops Planners knowledge set with targeted knowledge and skills related to tactics, techniques, procedures, cyber threats, and operational planning in offensive cyber operations. It provides a more detailed and focused subset of competencies within

the broader cybersecurity and network operations field described in the NICCS Cyber Ops Planners knowledge set.

The literature review results and the NICCS Cyber Ops Planners' knowledge devised the knowledge list. These provide a more targeted and specific subset of competencies within the broader cybersecurity and network operations field described in the NICCS Cyber Ops Planners knowledge set. It refines and specifies the requirements for OCO planners. The specific contributions of new knowledge are knowledge of the cyber centre of gravity (a critical point—a source of power for the adversary's cyber operations); they can target it (Smart 2011) and cyberweapon(s) deployment and reuse periods (shelf-life) (Lidestri 2022).

The existing NICCS Cyber Ops Planners' knowledge set was refined through a comprehensive understanding of various crucial aspects. These included cyber threats (Barber et al. 2016), cyberspace operations (Bender 2013), core competencies and professional networking [6]. Additionally, they delved into intelligence collection capabilities (Barber et al. 2016), joint functions and operational procedures (Bender 2013). This knowledge was further enriched by exploring the kill chain framework (Barber et al. 2016), and cyber threats analysis (Neville et al. 2020).

3.3 Skillset

These results contribute to NICCS Cyber Ops Planners' skills by providing a more specialised and detailed set of skills and abilities related to cyber operations. While NICCS Cyber Ops Planners skills focus on administrative and planning activities, the results delve deeper into cyber operations' cognitive and technical aspects. These skills, such as cyber intelligence analysis (Neville et al. 2020), targeting (Smart 2011), analytical skills (Mulford 2013), and technical planning (Barber et al. 2016), provide a more specific and comprehensive understanding of the competencies required for effective cyber operations planning.

Incorporating the results into NICCS Cyber Ops Planners skillsets enriches the overall competency profile, offering a more holistic view of the skills needed for Offensive Cyber Operations planners. It provides a bridge between administrative and planning activities and the technical and cognitive aspects of cyber operations, ensuring that planners are well-equipped to address the multifaceted challenges in the cyber domain. The merged skills list provides a comprehensive set of competencies covering administrative planning and the technical aspects of offensive cyber operations, offering a well-rounded view of the skills required for Offensive Cyber Operations planners.

3.4 Abilities

This systematic review contributes to NICCS Cyber Ops Planners' abilities by providing a more specialised and detailed set of abilities and cognitive skills related to cyber operations planning. While NICCS Cyber Ops Planners' abilities focus on general communication and collaboration skills, the systematic review inquires more profoundly into the abilities required for effective coordination in offensive cyber operations. The cognitive skills introduced in the Manual of Navy Enlisted Manpower and Personnel Classifications and Occupational Standards (Navy Personnel Command 2023), such as

deductive reasoning, originality, and problem sensitivity, provide a more comprehensive understanding of the competencies needed for complex problem-solving in the cyber domain.

Assembling current review abilities into NICCS Cyber Ops Planners' abilities enriches the overall competency profile, offering a more holistic view of the knowledge, skills, abilities, and experiences required for cyber operations planners. It bridges the gap between general communication and collaboration skills and the specialised abilities necessary for successful planning and coordination in the cyber operations field.

This review contributed to the additions to the NICCS Cyber Ops Planners' abilities, such as the ability to lead joint operations and develop cyber capability, doctrine, and tactics. Ability to conduct offensive cyber operations effectively (Withers 2018). Abilities for ongoing intelligence gathering and planning to deter or defeat cyber-attacks (Barber et al. 2016). Communication abilities, such as written and -oral expression. Abilities in Deductive Reasoning, Originality, Inductive Reasoning, Problem Sensitivity, Information Ordering, Fluency of Ideas and Selective Attention (Navy Personnel Command 2023).

3.5 Experience

Individuals in the Cyber Planner work role typically possess a diverse skill set gained from hands-on experience in multiple Cyber Mission Force roles encompassing defensive and offensive operations. This practical experience extends to the development and execution of cyber operation plans, demonstrating their proficiency in translating strategic objectives into actionable tactics within the cyberspace domain. Moreover, these professionals have a comprehensive understanding of the intricacies of the cyber realm, including its lexicon, authorities, guidance, organisational structures, and command relationships. They leverage this knowledge to navigate the complex landscape of cyberspace operations planning and to make informed decisions that align with strategic objectives. Their expertise extends to the core competencies of cyberspace operations, which include professional networking, social collaboration, and information systems technology. These competencies facilitate effective communication and cooperation within and beyond cyberspace. Furthermore, individuals in this role are well-versed in joint functions and operational procedures, allowing them to integrate cyberspace operations into broader military strategies seamlessly. They excel in the development and execution of operational plans, ensuring that they align with broader military objectives and are executed efficiently. In addition to practical experience, they have a background in military education, training, and certifications, which underscores their commitment to continuous learning and professional development. The proficiency they achieve is the result of several years of dedicated experience in the field, making them highly qualified and effective in their roles as Cyber Planners.

4 Discussion

This paper's objective was to define the role of an operational-level OCO planner. The operational skills, digital skills, soft skills, and experience required for the competencies needed in the operational-level OCO planner were identified. This enabled a framework

to be devised, including a training plan, required skillsets, and all necessary competencies to become a practical OCO planner.

Initially, the role of an operational-level OCO planner was defined. The literature revealed four definitions. In summary, while all definitions describe a Cyber Operations Planner's role, they differ in emphasis. The first definition focuses on collaboration and execution, the second on broad functions and experience, the third on mission analysis and coordination, and the fourth on monitoring and compliance. Only the NIST Frameworks definition includes the targeting, a unique attribute for OCO planners. Together, they provide a comprehensive view of the responsibilities and skills of the Cyber Operations Planner role.

The literature led us to identify new knowledge, skills, abilities, and experience required for the competencies needed in the operational-level OCO planner. The summary of identified knowledge, skills, abilities, and experience is presented in Table 4. Considering the small amount of available literature and despite the existing OCO planner's NICCS framework, this significantly contributes to defining an OCO planner's competencies.

An essential skill of OCO planners is the analysis of network metadata (Mulford 2013). A significant part of operational planning takes place in the logical layer. The logical and cyber-persona layers are interconnected, with state borders affecting hardware components' geographical positions. They consist of code or data entities, allowing communication and action between the physical and cyber-persona layers. COs occur at the logical layer (AJP-3.20 2020, pp. 3,17). Additionally, to achieve the intended result by cyber methods, logical and physical targets must be considered simultaneously (Arik et. al. 2022). To grasp the logical layer, planners must have the ability to understand and analyse network data. Otherwise, planning will suffer, and the entire mission may be at risk.

The critical knowledge identified was the deployment and reuse periods(shelf-life) of cyber weapons (Lidestri 2022). This is a unique and critical knowledge that very few publications have addressed. For example, a recent Rand Corporation report suggested planning, budgeting, and collecting historical data to procure cyberweapons. The research underscored the growing value and demand for specific exploits, particularly in mobile platforms, messaging apps, and specific zero-click and remote exploit categories. It also depicted the shifting landscape where Android exploits gained prominence over iOS, evidenced by the dramatic increase in Android value from 2015 to 2019 (Rand Corporation 2023).

Another required knowledge is about the adversary's source of power (Smart 2011). OCO planning involves identifying the cyber centre of gravity and establishing boundaries for joint operations. Targeting aligned with the cyber centre of gravity minimises the potential for lateral damage and effects.

A specific skill for OCO planners is targeting. Targeting involves knowledge, skills and tasks (NICCS 2023). Together, these lead to assessing vulnerabilities and capabilities, using intelligence to counter potential actions, and collaborating across different entities to create effective strategies to address or neutralise potential threats. Additionally, the NICCS Cyber Ops Planners Work Role described the Task, which was outside this paper's scope but provided a vast overview of activities needed for OCO planners.

A solid background in doctrinal joint functions and operations procedures is necessary for cyberspace operations planners. (Bender 2013). This is critical to breaking down the barriers between traditional and cyber operations, advocating for a shared understanding, collaboration, and integration between these two spheres for more effective joint military endeavours.

To become a practical OCO planner, self-learning is encouraged to build professional skills, including cyber domain expertise, professional reading, blogs, societies, conferences, videos, podcasts, and training sources (Bender 2013). This is supported by the NICCS Cyber Ops Planners Work Role Capability Indicators, which recommend 40 h annually of mentoring, shadowing, conferences, webinars or rotations (NICCS 2023). Cyber domain expertise can be gained through NATO CCDCOE-organised exercises such as Locked Shields[4] and Crossed Swords[5]. The Locked Shields exercise pits Red and Blue teams in handling large-scale cyber incidents, requiring effective reporting, strategic decision-making, and forensic, legal, and media challenges. The Crossed Swords exercise includes leadership training for the command element(planners) and joint cyber-kinetic operations. These exercises provide an excellent opportunity to obtain DCO and OCO proficiency to become a practical OCO planner.

This work also proposed a training plan that covers advanced cyber warfare, network attacks, operations, information security, troubleshooting, and risk management. It equips individuals with the necessary skills for effective OCO planning. One must complete civilian and military education and training to acquire the skills required to become a proficient OCO planner.

5 Limitations and Future Work

The reviewed literature had several limitations. A few of the sources were not subjected to peer assessment. For example, master‘s theses (Curnutt and Sikes 2021), (Houston 2019) and (Lidestri 2022). However, these are scholarly sources due to their close supervision, academic audience, extensive research, research methodology, and citation in other scholarly work.

Several sources needed to be more scholarly in nature. One such instance is the contract with the U.S. General Services Administration (U.S. General Services Administration 2022). Since the contract is a governmental arrangement, one can assume that audits have been conducted. This contract also provided insightful information that helped define the Cyber Operations Planner. Another helpful document was the Manual of Navy Enlisted Manpower and Personnel Classifications and Occupational Standards as Chapter 20 (Navy Personnel Command 2023). This paper was beneficial in outlining the competencies of Cyber Operations Planners.

The search terms related to offensive cyber operations planners' competencies may limit the research scope, as they may need to be narrower and specific. The terms "cyber operations competencies" and "cyber operational planner" vary in detail, and some terms may yield redundant information due to their similarity. Few articles on offensive

[4] https://ccdcoe.org/exercises/locked-shields/.

[5] https://ccdcoe.org/exercises/crossed-swords/.

cyberspace operations competencies are published due to secrecy, security concerns, legal and ethical considerations, and public disclosure incentives.

For future work, expert interviews with persons who have completed the task themselves should be used to validate the suggested framework in subsequent studies. Lastly, contact Cyber Command's human resources to learn how long it takes to educate an offensive operation planner.

6 Conclusions

The Offensive Cyber Operations competencies required for operational planning have yet to be fully documented and are significantly lacking compared to those for defensive cyber operations. We found only one framework for Offensive Cyber Operations competencies for operational planners. The National Initiative for Cybersecurity Careers and Studies Cyber Ops Planner's work role provided the foundation for this paper's new framework development. This paper resulted in a Framework for Offensive Cyber Operations Planners, which benefits Cyber Headquarters operational planners' training and development plans. As well as the proposed framework can contribute to preparing and planning NATO cyber operations exercises. Standards for offensive operations roles, definitions and competencies must be developed and implemented in studies.

To conclude, the experience required for an OCO planner typically possesses a combination of practical experience and knowledge. These include experience in multiple cyber operations in various defensive and offensive roles. The development and execution of cyber operations plans require an understanding of cyber-related terminology and structures and proficiency in cyberspace core competencies. These should be combined with a familiarity with joint functions and operational procedures and a military education, training, and certifications background. This expertise is typically acquired over several years of experience in the field.

Acknowledgements. The EU Horizon2020 project MariCybERA (agreement No 952360) funded research for this publication. We also thank Dr Cate Jerram from the University of Adelaide.

References

AJP-3.20. Allied joint doctrine for cyberspace operations. Nato Standardization Office (NSO) (2020). https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320

Arik, M., et al.: Planning cyberspace operations: exercise crossed swords case study. J. Inf. Warfare **70** (2022)

Barber, D.E., et al.: Cyberspace operations planning: operating a technical military. Military Cyber Aff. **1**(1), 3 (2016)

Bender, J.M.: The cyberspace operations planner. Small Wars J. **16** (2013)

Bendler, D., Felderer, M.: Competency models for information security and cybersecurity professionals: analysis of existing work and a new model. ACM Trans. Comput. Educ. **23**, 1–33 (2023)

Caton, J.L.: Implications of Service Cyberspace Component Commands for Army Cyberspace Operations. USAWC Press, Carlisle (2019)
Chowdhury, N., Gkioulos, V.: Key competencies for critical infrastructure cyber-security: a systematic literature review. Inf. Comput. Secur. **29**, 697–723 (2021)
Curnutt, A.J., Sikes, S.R.: Naval postgraduate school. Thesis - knowledge management application to cyber protection team defense operations (2021). https://apps.dtic.mil/sti/citations/AD1164246
ENISA. Information Operations – Active Defence and Offensive Countermeasures. ENISA (2016). https://www.enisa.europa.eu/topics/incident-response/glossary/information-operations-2013-active-defence-and-offensive-countermeasures
Houston, R.: Thriving Cybersecurity Professionals: Building a Resilient Workforce and Psychological Safety in the Federal Government. University of Pennsylvania, Pennsylvania (2019
Huskaj, G., Axelsson, S.: A whole-of-society approach to organise for offensive cyberspace operations: the case of the smart state Sweden. In: Proceedings of the 22nd European Conference on Cyber Warfare and Security, ECCWS 2023 (2023. https://pdfs.semanticscholar.org/b106/105500fcefd1d554a7dae6f06b2bd1d2c41a.pdf
Jensen, M.S.: Five good reasons for NATO's pragmatic approach to. Def. Stud. **465** (2022)
Joint Pub 5-0. Doctrine for Planning Joint Operations. Retrieved from Doctrine for Planning Joint Operations (1995). https://edocs.nps.edu/dodpubs/topic/jointpubs/JP5/JP5-0_950413.pdf
Joint Publication 1. Doctrine for the Armed Forces of the United States. Retrieved from Joint Doctrine Publications - Joint Chiefs of Staff (2013). https://irp.fas.org/doddir/dod/jp1.pdf
Jøsok, Ø., et al.: Self-regulation and cognitive agility in cyber operations. Front. Psychol. **10**, 410188 (2019)
Libicki, M.C., Tkacheva, O.: Cyberspace escalation: ladders or lattices? In: CCDCOE, Tallinn (2020)
Lidestri, M.R.: Incorporating perishability and obsolescence into cyberweapon scheduling, MONTEREY, California, U.S (2022
Moher, D., et al.: Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. Syst. Rev. **4**, 1–9 (2015)
Mulford, L.A.: Let slip the dogs of (cyber) war: progressing towards a warfighting US cyber command. Joint Advanced Warfighting School, Norfolk (2013)
National Institute of Health. What are competencies? Retrieved from Office of Human Resources (2023). https://hr.nih.gov/about/faq/working-nih/competencies/what-are-competencies
NATO CCDCOE. NATO CCDCOE Training Catalogue 2023 (2023). https://ccdcoe.org/uploads/2023/09/2023_NATO_CCD_COE_Training_Catalogue_final.pdf
NATO Standardization Office. Allied Joint Publication-3.20. Allied Joint Doctrine for Cyberspace Operations (2020). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf
Navy Personnel Command. Chapter 20 Cryptologic technician (Networks) (CTN). Navy Personnel Command (2023). https://www.mynavyhr.navy.mil/Portals/55/Reference/NEOCS/Vol1/CTN_occs_CH_95_Jul23.pdf?ver=CWQ8uOEoG-z0c7PLZqXKRg%3d%3d
Neville, K., et al.: United States Army Research Institute for the Behavioral and Social Sciences. A Cognitive Skills Research Framework for Complex Operational Environments (2020). https://apps.dtic.mil/sti/pdfs/AD1091744.pdf
NICCS. Cyber Operational Planning. National Initiative for Cybersecurity Careers And Studies (2023). https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/cyber-operational-planning
Nizich, M.: Emerald insight. The Cyberhero and the Cybercriminal (2023): https://www.emerald.com/insight/content/doi/https://doi.org/10.1108/978-1-80382-915-920231006/full/html

RAND Corporation. Educating for Evolving Operational Domains. RAND Corporation, California (2022)

Rand Corporation. A Cost Estimating Framework for U.S. Marine Corps Joint Cyber Weapons. Santa Monica: RAND Corporation. For more information on this publication (2023). www.rand.org/t/RRA1124-1

Shoemaker, D., Kohnke, A., Sigler, K.: A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0). CRC Press, Boca Raton (2016)

Smart, S.J.: Joint Targeting in Cyberspace. Washington, Pentagon, U.S (2011)

Tricco, A.C., et al.: PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation. Ann. Internal Med. **169**, 467–473 (2018)

U.S. General Services Administration. U.S. General Services Administration. General services administration Federal Supply Service Federal Supply Schedule Price List (2022). https://www.gsaadvantage.gov/ref_text/47QTCA22D00C8/0XKGIE.3TATEZ_47QTCA22D00C8_NNDATA47QTCA22D00C8A81509012022.PDF

United States Army War College. Strategic Cyberspace Operations Guide (2022). https://media.defense.gov/2023/Oct/02/2003312499/-1/-1/0/STRATEGIC_CYBERSPACE_OPERATIONS_GUIDE.PDF

Goździewicz, W.: Cyber Defense Magazine. Retrieved from Voluntarily by Allies (SCEPVA) (2019). https://www.cyberdefensemagazine.com/sovereign-cyber/

Withers, P.: Integrating cyber with air power in the second century of the royal air force. Royal Air Force Air Power Rev. **21**(3), 148–151 (2018)

Appendix 4

Publication IV

Arik, Marko; Lugo, Gregorio, Ricardo; Ottis, Rain; Venables, Adrian (2024). Optimising Offensive Cyber Operation Planner's Development: Exploring Tailored Training Paths and Framework Evolution. Frontiers in Computer Science-Computer Security.

frontiers | Frontiers in Computer Science

TYPE Original Research
PUBLISHED 07 June 2024
DOI 10.3389/fcomp.2024.1400360

OPEN ACCESS

EDITED BY
Saqib Saeed,
Imam Abdulrahman Bin Faisal University,
Saudi Arabia

REVIEWED BY
Jeremy Hilton,
Cranfield University, United Kingdom
Neda Azizi,
Torrens University Australia, Australia

*CORRESPONDENCE
Marko Arik
✉ marko.arik@taltech.ee

RECEIVED 13 March 2024
ACCEPTED 27 May 2024
PUBLISHED 07 June 2024

CITATION
Arik M, Lugo RG, Ottis R and Venables AN (2024) Optimizing offensive cyber operation planner's development: exploring tailored training paths and framework evolution. *Front. Comput. Sci.* 6:1400360. doi: 10.3389/fcomp.2024.1400360

Optimizing offensive cyber operation planner's development: exploring tailored training paths and framework evolution

Marko Arik [1]*, Ricardo Gregorio Lugo [2,3], Rain Ottis [1] and Adrian Nicholas Venables [1]

[1]Department of Software Science, Tallinn University of Technology, Tallinn, Estonia, [2]Estonian Maritime Academy, Tallinn University of Technology, Tallinn, Estonia, [3]Department of Welfare, Østfold University College, Halden, Norway

This study aims to investigate Offensive Cyber Operations (OCO) planner development, focusing on addressing the need for tailored training paths and the continuous evolution of frameworks. As the complexity of global challenges and security threats grows, OCO planners play a pivotal role in operationalising and executing operations effectively. The research utilized a qualitative case study approach, combining literature reviews and interviews with OCO military professionals, to explore OCO planners' competencies and training frameworks at the operational level. Interviews emphasize the need for comprehensive training, trust, and standardized training pathways in OCO planning, with real-time exposure being the most effective approach for practical planning. The literature review highlights key OCO training options, including Cyber Range Integration, cognitive architectures, and Persistent Cyber Training Environment platforms. It emphasizes educational initiatives, industry contributions, and practical experience in developing expertise in OCO. Discussions highlight the importance of Cyber Range Integration, educational initiatives, and practical experience in OCO. It emphasizes the need for a dual skill set and a structured training path for OCO planners. Real-time exposure through exercises and courses is the most effective approach to becoming a practical OCO planner.

KEYWORDS

cyberspace operations planning, cyberspace planners' competencies, Offensive Cyber Operations, training, Defensive Cyber Operations

Introduction

It is crucial to map the essential skills and competencies required for members of a military's Cyber Headquarters staff, particularly for Cyber Operations (CO) planners. Preparation of cyberspace operations (COs) requires planners to consider technical peculiarities irrelevant in planning traditional military operations (Barber et al., 2016). These individuals must possess military planning expertise and a deep understanding of cyberspace operations. Building a proficient Cyber team necessitates a clear comprehension of the mandatory skills and experiences for each role within the team (Jones, 2019). Cyber operations management occurs at three levels—strategic, operational, and tactical—each demanding specific skill sets (AJP-3.20, 2020). Situational awareness is crucial at the strategic level, technical skills are paramount at the tactical level,

and operational-level planning requires cognitive skills from commanders and their staff, supported by knowledge, experience, and judgment (Joint Publication 1, 2023).

This article examines the competencies required for Offensive Cyber Operations (OCO) planners at the operational level. Recognizing the factors influencing the performance of cyber operators is essential for enhancing the education and training of military cyber personnel (Jøsok et al., 2019). While it's known through experience that the competencies of Defensive Operations (DCO) planners differ from those of OCO planners, there is a lack of current research to validate this distinction (Jøsok et al., 2019). Existing research in cyber operations has predominantly concentrated on DCO, specifically at the tactical level. This article focuses on operational-level cyber planners' competencies and training frameworks, specifically emphasizing Offensive Operations (OCO). Given its scope and focus, legal and other competencies are not the primary areas of consideration.

The research reported here aims to apply academic rigor to identify the competencies required for OCO planners and verify them through expert interviews.

Several NATO countries increasingly acknowledge the utilization of Offensive Cyber Operations (OCO) planning. The 2016 NATO Warsaw Summit addressed OCO capabilities through the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA) mechanism. Despite NATO's longstanding policy of refraining from offensive actions in cyberspace and the absence of the Alliance creating offensive cyber capabilities, the SCEPVA mechanism serves as the exclusive avenue. Within this framework, operational-level commanders can request nations possessing cyber capabilities to execute offensive cyber effects against a specified target (Gozdziewicz, 2019). Organizing offensive cyberspace operations is necessary despite challenges such as human resource and skill requirements (Huskaj and Axelsson, 2023). In light of these considerations, this article emphasizes military aspects at the operational level and outlines training requirements relevant to cyberspace.

Differences in OCO and DCO

The distinctive capability of Offensive Cyber Operations to exert control within the operational domain starkly contrasts with the inherent limitations faced by Defensive Cyber Operations (DCO) in managing external infrastructures, a nuance well-documented within the literature (Barber et al., 2016; Jones, 2019). These differences are further accentuated by the OCO's reliance on intricate third-party infrastructures, which necessitates a multifaceted understanding of Operational Security (OPSEC) to effectively navigate the complex landscape of multiple controlling entities (AJP-3.20, 2020). The foundational aspect of OCO, characterized by the utilization of complicated Information and Communication Technology (ICT) infrastructure that is often leased and only partially controlled, diverges from the cybersecurity baseline of DCO, which is predicated on owned and entirely governed ICT infrastructure (Joint Publication 1, 2023). This divergence not only highlights the strategic offensive posture of OCO, aimed at manipulating target data, technology, and personnel, but also underscores the intricate challenges such as tool development, intelligence gathering, and navigating legal constraints that OCO planners must adeptly manage (Gozdziewicz, 2019; Jøsok et al., 2019). This illuminates the multifaceted and complex nature of OCO planning, emphasizing the criticality of comprehensive OPSEC understanding, adept management of third-party infrastructures, and the imperative for continuous training and international collaboration to bolster the effectiveness and strategic impact of military and cybersecurity organizations in the realm of cyber warfare.

Integration and information sharing between OCO and DCO

This subsection examines the benefits and challenges of combining information flows between DCO and OCO. Integrating OCO and DCO is pivotal in enhancing national and organizational cybersecurity frameworks. This combined effort allows for a proactive stance in cyber defense, anticipating and neutralizing threats before they manifest into breaches. As Libicki (2009) posits that an effective cyber strategy encompasses offensive capabilities to deter and disrupt threats and defensive capabilities to protect and respond (Libicki, 2009). As Nye (2017) discusses that effective cyber deterrence strategies often depend on the seamless integration of offensive capabilities that disrupt and dissuade adversaries, combined with defensive measures that protect critical infrastructures and respond to incursions.

Furthermore, the integration of these strategies ensures a more resilient infrastructure. As detailed by Andress and Winterfeld (2013), the tactical knowledge from offensive operations provides critical insights into potential vulnerabilities that could be exploited by adversaries, thereby enhancing defensive measures (Andress and Winterfeld, 2013). This comprehensive approach is supported by national strategies, as outlined in the U.S. Department of Defense's (2015) Cyber Strategy, which advocates for a seamless operation between offensive and defensive strategies to maintain superior cybersecurity capabilities.

State of the art

Understanding the competencies for planners of Offensive Cyber Operations (OCO) at the operational level within NATO Cyber Headquarters is crucial in today's digitally dependent world. As cyber threats evolve, effectively planning and executing OCOs becomes pivotal, especially within the NATO context and considering frameworks like the Sovereign Cyber Effects Provided Voluntarily by Allies (SCEPVA). Developing a deep understanding of these competencies through methods such as qualitative case studies, semi-structured interviews, and literature reviews is vital. This understanding enhances the effectiveness of NATO operations and contributes to the security and resilience of digital infrastructures in the face of sophisticated cyber threats. Focusing on operational-level planning within NATO's framework ensures that a specific and nuanced approach is vital for addressing contemporary cyber challenges.

Training frameworks for offensive cyberspace operations

This section concisely summarizes the current training frameworks for offensive cyberspace operations. By examining existing knowledge and practices, the aim is to offer insights into the conceptual foundations that underpin offensive cyber training.

The necessity for proficient professionals in Offensive Cyber Operations (OCO) has been acknowledged within the field. According to the Atlantic Council (2021), the efficacy of offensive cyber operations programs is contingent upon the individuals' expertise. Challenges encountered within industry, academic circles, and various governmental sectors differ from those faced during individual and collective training exercises for NATO cyber operations. Unfortunately, a need for more alignment exists between our forces' training requisites and the educational provisions currently available (Walcott, 2015).

Integrating training challenges with a hybrid approach in military cyber forces

The complexity and necessity of modern cyber warfare readiness are accentuated by integrating challenges within training environments, employing a hybrid approach to military cyber forces. Jones (2015) underscores the critical need for training environments to foster cyber warfighters' purposefulness, creativity, and adaptability, necessitating an effective integration with authentic cyber ranges. This integration facilitates seamless transitions across testing, evaluation, and training platforms, enhancing the realism and effectiveness of the training. This is supported by Walcott (2015), who identifies the inadequacies of relying solely on existing knowledge for training military cyber forces. A paradigm shift toward experiential learning, derived from cyber-warfighting experiences, is advised to address these inadequacies; thus, Walcott (2015) proposes that a hybrid approach featuring specialized teams with updated and adaptable capabilities emerges as a solution. However, the feasibility of this approach may be difficult due to the demanding design, planning, and execution skills required for effective cyberspace management. The foundation of skilled military cyber forces lies in effective individual and collective training, as emphasized by Walcott (2015). The operational experience plays a pivotal role in assessing the realism and effectiveness of current training methodologies. Such experience is indispensable for ensuring that training is aligned with real-world operations, thereby improving the success rate in cyber-based military engagements.

Advancements in cyber simulation and training

The evolution of training environments to include cognitive-level synthetic cyber offense and defense strategies is crucial, given the dynamic nature of cyber warfare. Jones (2015) highlights the importance of evolving training environments to encapsulate cyber warfighters' purposefulness, creativity, and adaptability. A vital aspect of this evolution is the integration of cognitive agents and the Soar architecture, which provides a robust framework for modeling attackers, defenders, and users within realistic cyber ecosystems (Jones, 2019). The Cyber Cognitive Framework (CyCog), leveraging the Soar architecture, exemplifies the practical and theoretical foundations for cognitive cyber operations modeling. This integration addresses critical shortcomings by providing real-time generative models capable of effective deployment in live network environments. The emphasis on cognition and integration presents a promising avenue for advancing research and development in cyber warfare training applications. While not directly referencing the Cyber Cognitive Framework (CyCog), other research has contributed to the understanding and application of cognitive principles within the realm of cybersecurity and digital transformation. Elia and Margherita (2022) provide a conceptual framework for cognitive enterprises, emphasizing the integration of advanced cognitive technologies to enhance organizational capabilities, which parallels the objectives of CyCog in leveraging cognitive approaches for cybersecurity. McNeese and Hall's (2017) work on the cognitive sciences of cyber-security proposes a framework to advance socio-cyber systems, aligning with CyCog's focus on applying cognitive principles to improve cyber defense mechanisms. Khanna's (2019) exploration of a cognitive education framework for cyber security, though not directly related to CyCog, suggests complementary educational approaches that could inform the development of cognitive capabilities within the cybersecurity domain. Lastly, the proposal by Tayeb et al. (2018) for a cognitive framework to secure smart cities through the use of deep learning to predict security breaches resonates with CyCog's aim of employing cognitive frameworks to anticipate and mitigate cyber threats. These articles highlight the significance of cognitive approaches in enhancing cybersecurity measures, educational strategies, and organizational resilience, providing a broader context for understanding and appreciating the potential impact of frameworks like CyCog in the cyber domain.

Persistent cyber training environment and offensive cyber capabilities support

The Persistent Cyber Training Environment, initiated by the Army in 2016, underscores the importance of a dedicated platform for training, assessment, and mission rehearsal in cyber warfare. This environment is instrumental in major cyber training exercises, such as Cyber Flag, and supports nearly 9,000 users across all military departments (GAO, 2022). Integrating artificial intelligence and machine learning within this program signifies the growing emphasis on advanced technological solutions to enhance cyber warfighter readiness. Supporting the proliferation of Offensive Cyber Capabilities (OCC) is anchored in key pillars, including educational initiatives and establishing connections among skilled professionals.

The concept of Offensive Cyber Capabilities (OCC) is anchored in multiple strategic dimensions that redefine how states can use military power (Herrick and Herr, 2016; Smeets, 2018; Smeets and Lin, 2018). These strategic aspects provide a framework for

understanding the multifaceted role of OCC in modern military strategy and international security.

- Strategic Compellence and Deterrence: having OCC gives states the ability to influence adversaries through cyber operations without necessarily exposing these actions publicly. This can, for example, allow for the de-escalation of conflicts as the compelled party can comply without public acknowledgment of coercion. OCC's role in deterrence, particularly among states with credible reputations in cyber capabilities, can influence adversaries' decisions and behaviors (Smeets and Lin, 2018).
- Pre-emptive and preventive defense: the nature of OCC allows for both pre-emptive and preventive actions against potential cyber threats. This capability enhances a state's defensive posture by providing options to neutralize threats before they materialize into attacks, thereby contributing to the strategic use of military power in cyberspace (Smeets and Lin, 2018).
- Organizational integration and efficiency: integrating intelligence and military capabilities to develop OCC provides benefits such as enhanced interaction efficiency, better knowledge transfer, and reduced mission overlap. However, this integration also poses challenges such as cyber mission creep, the gradual broadening of the scope and objectives of cyber operations beyond their original intent, and potential escalation in the cyber security dilemma, where defensive measures taken by one state in cyberspace can be perceived as threatening by another state, prompting the latter to respond with its own cyber defensive and potentially offensive measures (Smeets, 2018).
- Operational complexity and cost-effectiveness: the development and deployment of OCC involve complex design and execution processes that are both resource-intensive and vulnerable to countermeasures. Therefore, OCC's strategic value must be weighed against these operational complexities to ensure cost-effective cyber-capabilities investments (Herrick and Herr, 2016).
- Symbolic value and international prestige: while the tangible effects of OCC can be significant, its symbolic value as a "prestige weapon" remains unclear due to cyber operations' largely non-material and transitory nature. The prestige associated with possessing advanced OCC can influence international relations and perceptions of military power (Smeets and Lin, 2018).

This approach is evident in various sectors, from government institutions like the US National Security Agency National Cryptologic School to industry contributions and Access-as-a-Service examples (Atlantic Council, 2021). The proliferation of Offensive Cyber Capabilities (OCC) is supported by educational initiatives and professional networking in various sectors, as evidenced by the following research findings:

- The assessment of offensive cyber capabilities highlights the critical importance of cybersecurity in the face of growing threats and the need for countries to understand and develop their capabilities. This involves recognizing the talent behind cybersecurity as a critical indicator for assessing offensive capabilities (Selján, 2023).
- Offensive cyberspace operations, including "Offensive Defense," emphasize the strategic approach of taking the fight to the adversary, necessitating a comprehensive understanding of cyber operations and the importance of doctrine, training, and education in this domain (Dekić, 2022).
- The need for skilled cybersecurity professionals is underlined by the challenge of teaching cyber defense, which requires practical skills underpinned by a solid theoretical understanding. Effective education and training are strategic factors in building a capable cybersecurity workforce (Dekić, 2022).
- The establishment of connections among skilled professionals is crucial for advancing cybersecurity education across all disciplines and levels, aiming to increase involvement and advancement of cybersecurity education to address the widespread need for cybersecurity awareness and skills (Ahmad et al., 2022).
- Supporting the proliferation of OCC through educational initiatives and professional networks is crucial for developing and maintaining strong cybersecurity capabilities across sectors. These efforts create a skilled workforce capable of addressing and mitigating cyberspace's complex and evolving threats.

Military cyber training programs and transition to enhanced capabilities

The establishment of specialized military cyber training programs, such as the U.S. Army's Cyber Leader Course, addresses the growing demand for qualified cyber leaders capable of navigating the complexities of cyberspace in operational domains (Conti et al., 2014). These programs aim to equip cyber warriors with a comprehensive understanding and capabilities for planning and executing cyber operations, reflecting the necessity of integrating advanced cognitive-level simulations and military structure to counter evolving cyber threats. The shift from the online black markets to official and state-backed organizations represents a significant step forward in the power to launch cyber-attacks. This change means requiring skilled teams to carry out these cyber-attacks. It highlights how crucial it is to properly train the people involved, whether they are initiating the attacks, the ones identifying weaknesses in computer systems, or the ones creating harmful software (Atlantic Council, 2021).

Practical training options and the future of cyber warfare readiness

Practical training options, such as the Crossed Swords exercise, provide invaluable experience in offensive cyber operations, encompassing leadership training, legal aspects, and joint cyber-kinetic operations (ACT NATO, 2023). These exercises offer a comprehensive training environment that goes beyond theoretical knowledge, preparing planners and cyber command specialists for the realities of modern warfare. Integrating cyber ranges,

utilizing advanced cognitive architectures like Soar, and employing platforms such as the Persistent Cyber Training Environment collectively contribute to developing expertise in cyber warfare. These initiatives, coupled with the emphasis on Offensive Cyber Capabilities and practical exercises like Crossed Swords, pave the way for a future where cyber forces are well-prepared to meet and overcome the challenges of emerging cyber threats.

Objectives

This research is essential for enhancing operational readiness, addressing strategic shifts in cyber warfare, closing knowledge gaps and supporting training initiatives. By shedding light on the competencies of OCO planners, this research contributes to the broader discourse on cyber warfare. The study's objectives encompass identifying key competencies, validating them through expert interviews, addressing research gaps, informing training initiatives, and contributing to strategic preparedness in military cyber operations. Some gaps and areas need to be adequately explored in the literature on OCO planning, including the distinct competencies of OCO planners. The operational-level focus of research is the validation of competencies. Further exploration of these areas is essential to enhance our understanding of OCO planning and inform training, education, and cyber operations.

Methods

Our research adopted a qualitative case study approach, marked by an iterative process integrating literature reviews and interviews. While our initial step involved a comprehensive literature review, our choice of a qualitative case study method is unconventional, underscoring the unique demands of our study on OCO planning at the operational level. This approach, characterized by integrating literature reviews and semi-structured interviews, was carefully selected to align seamlessly with the objectives of the article. The resulting mixed methods approach allows for a more holistic exploration of OCO planners' competencies and training frameworks, leveraging the strengths of qualitative case study methodology and insights from relevant literature and interviews. The selection process for interview participants was carefully designed to ensure a comprehensive representation of experiences across different NATO countries. This diversity is critical as it allows the research to cover a broad spectrum of perspectives regarding cyber operations planning and execution within the alliance.

Qualitative case study

Thematic analysis (Braun and Clarke, 2006), employed as a qualitative research method, systematically identifies, analyses and reports recurring patterns or themes within the data. Throughout the process, thematic analysis is iterative, meaning researchers move back and forth between different stages, refining their understanding of the data and the emerging themes. It is a flexible approach that allows for exploring complex and nuanced aspects of the data, ultimately leading to a rich and insightful interpretation of the research findings. Applied in the explorative study on OCO planners' competencies, this approach facilitates discovering and comprehending nuanced aspects of their skills and capabilities. By uncovering underlying meanings, thematic analysis contributes to a comprehensive understanding of the subject matter. The study combines theoretical frameworks with practical insights from semi-structured interviews to understand the competencies needed for Offensive Cyber Operations planners at the operational level. Participants were chosen based on their firsthand experience, ensuring a comprehensive understanding of the skills needed for operational planning.

Interview procedures

This study experiments with NATO's Crossed Sword exercise staff structure, which can handle the planning and management of complex OCO in real-time. Crossed Sword is a well-established cyber exercise; our data, findings, analysis, and developed framework will attract the interest of previous participants. This study employed semi-structured interviews as a critical methodological approach to gather insights from NATO OCO professionals. The interviewees were selected due to their practical experience in OCO planning. The objective was to comprehensively understand the multifaceted competencies and skills essential for effective OCO planning, encompassing technical, operational, and strategic dimensions.

The data collection process for interviews involved using secure digital videoconferencing platforms, where interviewees signed informed consent forms before the interviews. Interviewers posed pre-defined questions related to OCO planning, recorded responses, and cross-verified them with recordings for accuracy. The finalized data was sent back to interviewers for final verification. The structured interview guide ensured a comprehensive exploration of OCO planning competencies while allowing flexibility for diverse insights. This method ensured confidentiality, accuracy, and reliability in gathering insights into essential OCO planning skills and competencies.

Analysis and synthesis

Through a comprehensive examination of both existing offensive cyberspace training frameworks and insights obtained from the semi-structured interviews, we combined and synthesized the results. This synthesis unveils an appreciation of the competencies indispensable for Offensive Cyber Operations planners at the operational level. Integrating theoretical frameworks with practical insights ensures a holistic and nuanced comprehension of the skills and expertise required in this domain.

We specifically selected participants for our research based on their firsthand and hands-on experience organizing and carrying out offensive cyberspace operations (OCO). This deliberate hiring approach sought to obtain honest thoughts and viewpoints from people working in the field, guaranteeing a sophisticated comprehension of the skills needed for operational OCO planning.

Qualitative data analysis will use Braun and Clarke's (2006) six-step thematic analysis, engaging thoroughly with the data through multiple readings and developing initial impressions noted in a mind map. To ensure the validity of the qualitative data collection and analysis, Flick's (2019) approach for a comprehensive understanding of validity that encompasses both the production and presentation of data and Tracy's (2010), eight critical points for ensuring validity in qualitative research (a worthy topic, rich rigor, sincerity, credibility, resonance, significant contribution, ethics, and meaningful coherence) will be adapted. This research, addressing the OCO capabilities, emerges as a worthy topic due to its significant implications for cyber operations. The methodological approach of this study embodies rich rigor through the engagement with a diverse array of sources, as advocated by Weick (2007), ensuring a multifaceted understanding of the subject matter. The sincerity of the research process is maintained through the principal investigator's self-reflexive transparency regarding their professional background and its influence on the research, thus lending credibility to the findings. The resonance of the research is achieved through the effective communication of findings to a broad audience, facilitated by the use of clear, jargon-free language and supported by the diverse backgrounds of the study participants, enhancing the generalizability and transferability of the insights gained. This comprehensive approach to validity, encompassing the detailed criteria set forth by Tracy (2010) and aligned with Flick's (2019) perspective, underscores the study's adherence to rigorous qualitative research standards, thereby ensuring its contribution to the mental health domain in elite sports.

Ethics

The research discussed in the article operates within the framework of the lead author's PhD studies at TalTech, adhering to the university's Academic Ethics Principles. Ethical standards are upheld throughout the research process, including obtaining informed consent, ensuring secure digital communication channels, and verifying participant identities. Data is processed and stored securely within the academic environment and responsibly destroyed after publication to protect participant privacy and maintain research integrity. Following the terms of the interview informed consent agreements, the nationalities of the interviewees are kept confidential. This measure ensured that responses could be candid and the participants' privacy was fully respected.

Interviews

Semi-structured interviews were used to interact with NATO OCO experts to thoroughly examine the competencies and skills essential for efficient OCO planning. This method provides depth and flexibility, enabling a dynamic discussion that can include operational, technical, and strategic topics. Semi-structured interviews, with their personalized and open-ended framework, are beneficial for gathering contextual and nuanced information by utilizing the participants' expertise.

TABLE 1 The summary of Demographic Information of Interviewees.

Pseudoname	Background	Interview time
Interviewee A	A military veteran with a cybersecurity master's degree, has experience in operational-level CO planning exercises as the chief of operations planning.	02/02/2023
Interviewee B	Has technical and national CO planning experience, integrating cyberspace considerations into operational planning.	13/02/2023
Interviewee C	A cyberspace graduate is currently planning operational exercises like Locked Shields and Crossed Swords, holding a senior officer rank in military operational planning competence.	31/01/2023
Interviewee D	Has 23 years of military experience, including 5 and a half years in Cyberspace Command and NATO Authority, and is currently responsible for CO planning, doctrine development, and research.	02/02/2023
Interviewee E	With a master's degree in military and strategic planning, has experience in Joint Operational Planning and has been appointed as Deputy Director for the National Security Operations Center.	09/03/2023

Interview guide

The study developed questions 2–5 on competencies, skills, objectives, and training recommendations for OCO planners through a methodical process, including research objectives, literature review, expert consultation, and understanding of OCO planners' roles. The questions were refined, pilot-tested, and ethically integrated for comprehensive insights.

We conducted the interviews in semi-structured form. Under the signed informed consent form, the interviewer's identity and country of origin remain undisclosed.

We divided the semi-structured interviews into five main topics:

1. Background and experience of the interviewee.
2. What competencies are required in the given role?
3. What skills are involved are required for each of those competencies?
4. What are the objectives of the OCO planner?
5. Where are the recommendations for obtaining the best training and experiences?

Table 1 represents the summary of Demographic Information of Interviewees.

Results

The thematic analysis of interviews with experts in Offensive Cyber Operations (OCO) has revealed six pivotal themes in understanding the landscape of OCO planning. These themes encompass the essential differentiation between traditional kinetic and cyber operations, highlight the specialized competencies and skills necessary for effective OCO planning, and outline the objectives and responsibilities that OCO planners must navigate. Additionally, the analysis provides insights into the training recommendations tailored for OCO planners, identifies the multifaceted challenges inherent in OCO planning, and underscores the paramount importance of practical experience and exposure in this domain. These themes offer a comprehensive overview of the critical elements that define and shape OCO planners' role in modern cyber warfare.

The first identified theme is the necessity of distinguishing between kinetic and Cyber Operations. This theme emerged from statements made by the interviewees: *"The importance of understanding the differences between kinetic and cyber operations."* (Interviewee A); *"Acknowledge the unique time requirements of cyber operations."* (Interviewee B); and "*The difficulty of obtaining OCO experience and training at the unclassified level."* (Interviewee E). These insights highlight an essential distinction between kinetic and cyber operations. One must comprehend the divergent nature of cyber operations, as opposed to traditional kinetic military operations, emphasizing that cyber operations unfold in an ambiguous realm with effects that may not be immediately observable (Interviewee A). This divergence extends to the temporal dimensions of planning and execution, where cyber operations demand an understanding of their unique temporal requirements that can be instantaneous or dormant over long periods, challenging conventional paradigms of operational timing (Interviewee B). Compounding these distinctions is the challenge posed by the restricted environment in which cyber operational training and experience acquisition are confined, predominantly due to the classified nature of such activities, thereby complicating the practical preparedness of planners in this nuanced field (Interviewee E). Collectively, these insights highlight the need for a nuanced understanding and approach in planning and executing cyber operations, distinct from traditional kinetic strategies.

Another theme from the interviews is OCO planners' competencies and skills. Interviewee A notes the competencies of OCO planners in "*Understanding various stages within military operational planning.*" Interviewee B supported this and stressed the importance of OCO planners possessing "*Fundamental military operation aspects*" and "*Prior technical cyberspace-specific skills*." Interviewee C identifies "*Military planning skills*" and "*Proficiency in cyber intelligence*" *as necessary for OCO planners."* These statements highlight a critical theme that underscores the need for diverse competencies and skills in offensive cyber operations (OCO) planning. They emphasize a deep understanding of traditional military operational planning stages and stress the importance of integrating fundamental military principles with specialized technical knowledge specific to the cyber domain. Furthermore, the emphasis on military planning skills alongside proficiency in cyber intelligence underscores the necessity for OCO planners to possess a comprehensive skill set that marries strategic military insights with technical cyber capabilities.

Another theme that arose from the interviews was the objectives and responsibilities of OCO planners. Interviewee A identifies OCO planners' objectives as "*creating actionable plans aligned with higher-level commanders' expectations*." Interviewee D emphasizes the objectives of OCO planners to "*support multidomain military operations" and "enable and integrate OCO into joint planning.*" Interviewee E mentions "*the responsibility for OCO planning at the NATO level, involving collaboration with various functional areas.*" The statements support an understanding that the objectives and responsibilities designated for OCO planners include framing a comprehensive thematic understanding. Interviewee A's insight that planners aim to formulate actionable plans in harmony with the anticipations of higher-level commanders shows the critical alignment between operational planning and overarching strategic goals. Further elaborated by Interviewee D, the objectives extend to support multi-domain military operations and integrate OCO as a necessary aspect of joint planning. This highlights the role of cyber operations in contemporary military strategy. Moreover, Interviewee E's statement further highlights the collaborative nature of OCO planning, especially within a NATO context, where synchronized effort across diverse functional areas is needed, underpinning the multifaceted responsibilities of planners in a transnational alliance framework. These perspectives underscore the need for OCO planners to navigate a complex landscape of strategic alignment, integration, and collaboration to fulfill their roles effectively.

The next theme is training recommendations for OCO planners. Interviewee A recommends OCO planner training, starting with "*private companies' hacking courses and operations planning courses.*" Interviewee B highlights the need for "*more focused OCO courses at various levels*." Interviewee D recommends prioritizing "*operational planning, exercise planning, project management, and intermediate-level cyberspace technical training.*" These statements underscore the imperative for a structured and layered training approach for OCO planners. This includes having multifaceted learning trajectories and specialized OCO courses tailored to various proficiency levels to support a learning curriculum that evolves in complexity and depth. These statements also emphasize the importance of operational and exercise planning, project management, and technical training to capture the broad spectrum of skills required for adept OCO planning. This depends on a comprehensive educational strategy integrating tactical understanding with technical knowledge.

The next theme is challenges in OCO planning. Interviewee E mentions challenges in OCO planning, including "*long lead times, tool development, and intelligence gathering.*" Interviewee D identifies challenges in OCO planning, emphasizing the importance of "*trust among allies*" and "*joint training for OCO preparation*." Interviewee B highlights the complexity of OCO planning, recognizing "*legal constraints in certain NATO member states.*" The interviewee's experiences show that there are logistical and preparatory hurdles in OCO planning, such as extended lead times, the intricate process of tool development, and the critical need for effective intelligence gathering, which prolong the planning phase and complicate execution timelines.

They also highlight the relational and collaborative aspects by underscoring the necessity of trust among allied forces and the imperative for joint training initiatives to bolster OCO preparedness. Furthermore, there are legal issues where the various legal frameworks within NATO member states add a layer of complexity to OCO planning due to differing national regulations. Together, these insights portray the intricate tapestry of logistical, collaborative, and legal challenges that OCO planners must navigate.

Finally, The final theme is—the importance of practical experience and exposure. Interviewee E highlights the difficulty of obtaining OCO experience and training at the unclassified level. Interviewee D stresses the importance of "trust among allies" and "joint training for OCO preparation." Interviewee A emphasizes the importance of a "practical OCO planner development framework." These insights identify the challenges of accessing meaningful training and experiential learning opportunities outside classified environments. To gain access to meaningful experiences, trust-building among allies and the necessity of joint training exercises rely on collaborative and practical experiences that are fundamental for effective OCO preparedness. Therefore, structured development frameworks for OCO planners that prioritize practical, real-world experience are needed.

These themes illuminate the skills, difficulties, and training requirements OCO planners face and demonstrate the complex nature of offensive cyber operations planning.

Summary of key competencies and training requirements

The development of OCO planners is crucial for maintaining cybersecurity. Key competencies include technical acumen, strategic thinking, and leadership. This work helps align professional development with best practices and emerging cyber capabilities. The Key Competencies and Training Requirements are summarized in the Table 1.

Table 2 lists competencies with training requirements based on industry standards, academic research, and operational insights for future-ready OCO planners, ensuring comprehensive development.

TABLE 2 Key competencies and training for OCO planners.

Competency	Description	Required Training
Technical proficiency	Understanding of cybersecurity tools and techniques	Cybersecurity courses, cyber range exercises
Strategic thinking	Integration of cyber ops with military strategies	Strategic planning courses, wargaming
Operational planning	Execution of complex cyber operations	Workshops on cyber warfare operations
Ethical and legal understanding	Knowledge of laws governing cyber activities	Courses on cyber law and ethics
Interpersonal and leadership skills	Leadership and team management skills	Leadership programs, team-building exercises

General discussion

The literature review has contributed by outlining various key OCO training options. It emphasizes the importance of Cyber Range Integration, leveraging cognitive architectures like Soar and utilizing platforms such as the Persistent Cyber Training Environment for hands-on experience and skill refinement. Aligned with the first interview theme -the necessity of distinguishing between kinetic and Cyber Operations. OCO planners can gain practical, hands-on experience in simulated environments by integrating Cyber Range capabilities and leveraging cognitive architectures. This enables them to refine their skills, understand the nuances of cyber operations, and prepare for real-world scenarios effectively. Platforms like the Persistent Cyber Training Environment also provide a conducive space for continuous learning and skill development, contributing to OCO planning efforts' overall readiness and effectiveness. This is supported by previous research. These statements support the notion that OCO is ambiguous and often has non-immediate effects on cyber operations, contrasting with the direct physical impacts characteristic of kinetic operations, as Barber reported (Barber et al., 2016). This theme also points to the unique temporal dynamics of cyber operations, which may require instantaneous action or entail long-term, latent strategies, diverging from traditional operational timing paradigms (Jones, 2019; AJP-3.20, 2020). Previous findings address the challenges of acquiring practical experience and training in cyber operations due to the classified nature of such activities, which complicates the preparedness of planners in this complex field (Jøsok et al., 2019). Collectively, previous research and the statements provided by the experts underline the distinct nature of cyber operations and the critical need for specialized understanding and strategies distinct from those used in conventional kinetic military planning.

The review also indicates the significance of educational initiatives and industry contributions in supporting the growth of Offensive Cyber Capabilities (OCC) and the need for proficient teams in this domain. The theme "Training recommendations for OCO planners" highlights the importance of educational initiatives and industry contributions in developing Offensive Cyber Capabilities (OCC). Interviewee A recommends starting with private companies' hacking courses and operations planning courses, while Interviewee B suggests more focused OCO courses at various levels. Interviewee D emphasizes training in operational planning, exercise planning, project management, and intermediate-level cyberspace technical training. These recommendations align with the significance of educational initiatives and industry contributions in supporting the growth of OCC and the development of proficient teams. These expert insights are reinforced by findings from previous research that identify and discuss the critical role of educational programs and industry contributions in enhancing Offensive Cyber Capabilities (OCC). The Atlantic Council (2021) suggests the initiation of training with courses offered by private companies in hacking and operations planning, mirroring the recommendations for a comprehensive start in the field. Walcott (2015) further highlights

the necessity for specialized OCO training across various skill levels, advocating for a targeted approach to skill development in cyber operations. Also, the emphasis on a broader spectrum of training, including operational and exercise planning, project management, and technical skills in cyberspace, reflects the article's acknowledgment of the diverse competencies required for effective OCO planning (Jones, 2015). These aspects collectively highlight the identification and need for robust training frameworks that integrate both foundational and advanced skills, essential for cultivating proficient cyber operations teams and advancing OCC.

The interviews' last theme highlights the difficulties in gaining unclassified OCO experience, the value of mutual trust among allies, and the criticality of collaborative OCO preparation training. Interviewee A emphasizes the significance of a workable framework for developing OCO planners. The Crossed Swords exercise is the only publicly accessible OCO planning exercise in NATO. It emphasizes the importance of developing skills, encouraging teamwork, and dealing with the complexity of contemporary OCO situations. Previous research has also shown the importance of practical experience in OCO planning. The NATO Crossed Swords is identified as a real-world training environment deemed invaluable for OCO planners (ACT NATO, 2023). This exercise also addresses the challenges associated with acquiring unclassified experience in OCO, the indispensable value of trust among alliance members, and the necessity for joint training initiatives, as identified by the experts.

The adequacy of cyber integration into NATO's Intelligence Preparation phase underscores the alliance's proactive stance in adapting to the cyber-centric landscape of contemporary warfare, further illustrating how NATO's (2018) strategic commitments to enhancing cyber capabilities are being actualised in operational contexts. The alliance's proactive approach to adjusting to the cyber-centric nature of modern warfare is demonstrated by the adequate integration of cyberspace into NATO's Intelligence Preparation phase. This also demonstrates NATO's (2016) strategic initiatives to augment operational planning with cutting-edge cyber capabilities.

The emphasis on a structured developmental framework for OCO planners, as well as previous research and expert statements, agree with the need for a comprehensive training that builds individual competencies and fosters collaboration and adaptability in addressing the multifaceted nature of today's cyber operational landscape.

The literature review provides insights into diverse and comprehensive approaches for developing expertise in OCO, addressing current demands and future challenges in cyber warfare. In cyber operations (CO), the convergence of skill and tools is deemed essential, as more than skill alone is needed to confer the ability to plan effective operations. The significance of employing the right tools, incorporating procedures, and gaining experience were underscored as crucial components in developing operational capability. For individuals aspiring to engage in Offensive Cyber Operations (OCO), recommended courses, such as those offered by SANS,[1] were suggested to enhance proficiency. The theme about the competencies and skills of OCO planners aligns with the statement on the development of OCO expertise, meeting present needs, and upcoming difficulties in cyber warfare. Interviewees A, B, and C highlight that this theme includes understanding military operational planning stages, having basic military operation skills, having prior technical cyberspace-specific skills, having military planning skills, and being proficient in cyber intelligence, among other competencies and skills required of OCO planners. These proficiencies are highly compatible with the all-encompassing strategies emphasized in the literature study to cultivate OCO knowledge and meet the demands and difficulties of cyber warfare. Previous research supports that the competencies and skills essential for OCO planners are dependent on developing expertise in offensive cyber operations to address current and forthcoming challenges in cyber warfare. Specific competencies, such as a thorough understanding of military operational planning, foundational military operation skills, specialized technical skills in cyberspace, and proficiency in cyber intelligence, as pointed out by the respondents, resonate with the comprehensive approach outlined in the literature for developing OCO capabilities (Barber et al., 2016; Jones, 2019; AJP-3.20, 2020). This convergence of skills underscores the multifaceted nature of OCO planning, where a blend of strategic military insight and advanced technical knowledge is deemed crucial for navigating the complexities of modern cyber warfare and fulfilling the evolving demands and challenges posed within this domain.

Limitations

The limitations of this study primarily stem from its design and methodological choices. While adopting Braun and Clarke's (2006) thematic analysis facilitated a structured data exploration; this approach may also constrain the interpretation of data to pre-existing themes and potentially overlook emergent concepts not initially identified. Although valuable for in-depth understanding, the iterative nature of thematic analysis could introduce bias, particularly when the analysis is influenced by the researchers' preconceptions and the thematic framework they employ.

Another limitation is related to the objectivity of the research, as highlighted by Flick (2019) and Weick (2007). Given that both the interviewer and the interviewees are experts in Offensive Cyber Operations, there is a potential for shared biases to influence the data collection and analysis process. The five interviewed experts could have the same viewpoint, but these are considered top experts in NATO nations, and therefore, their knowledge and contribution are of significant relevance. The expert status of participants could lead to a convergence of viewpoints that might not fully encapsulate the diversity of perspectives within the broader field of OCO planning. While enriching the data with in-depth insights, this shared expertise might also narrow the scope of discussion and limit the exploration of alternative or contradictory viewpoints. Furthermore, while comprehensive, the focus on ensuring validity through Tracy's (2010) criteria may only partially mitigate the challenges of maintaining objectivity in a study where all involved parties have substantial expertise in the subject matter. The depth and richness of data from such a knowledgeable pool of participants are invaluable. Yet, it

1 https://www.sans.org/cyber-security-courses

inherently carries the risk of reinforcing existing paradigms without challenging or expanding them. This highlights the need for a critical reflection on the potential influence of the researchers' and participants' backgrounds on the research outcomes, necessitating continuous reflexivity throughout the research process to address and acknowledge these limitations.

Future research

Continuous research and development are crucial for developing sophisticated cyber tools, enhancing military network security, and training personnel to integrate cyber and kinetic operations. Understanding these integrations aids in crafting comprehensive defense strategies.

Conclusion

This study delves into Offensive Cyber Operations planning, highlighting key themes from interviews with experts in the field. These themes include the distinction between kinetic and cyber operations, the competencies and skills required of OCO planners, their objectives and responsibilities, training recommendations, challenges in planning, and the importance of practical experience.

Interviewees stress the need to understand the differences between kinetic and cyber operations, the diverse skills OCO planners must possess, and the challenges they face, such as long lead times and legal constraints. They also emphasize the importance of practical training and collaboration among allies.

The literature review reinforces these findings, emphasizing the significance of cyber range integration, cognitive architectures, and platforms like the Crossed Swords Exercise for hands-on experience. The study underscores the complexities of OCO planning and the continuous need for skill development and collaboration in cyber warfare.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Ethics statement

Ethical review and approval was not required for the study on human participants in accordance with the local legislation and institutional requirements. Written informed consent to participate in this study was provided by the patients/participants or patients/participants' legal guardian/next of kin.

Author contributions

MA: Conceptualization, Data curation, Formal analysis, Investigation, Methodology, Project administration, Resources, Visualization, Writing – original draft, Writing – review & editing. RL: Conceptualization, Methodology, Supervision, Validation, Writing – original draft, Writing – review & editing. RO: Funding acquisition, Supervision, Validation, Writing – review & editing. AV: Conceptualization, Project administration, Supervision, Writing – review & editing.

Funding

The author(s) declare that financial support was received for the research, authorship, and/or publication of this article. The EU Horizon2020 project MariCybERA (agreement No. 952360) funded research for this publication.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

ACT NATO (2023). *Retrieved from Exercise Crossed Swords Tests Allied Cyber Operations*. Available online at: https://www.act.nato.int/article/exercise-crossed-swords-tests-allied-cyber-operations/ (accessed June 15, 2023).

Ahmad, N., Laplante, P. A., DeFranco, J. F., and Kassab, M. (2022). A cybersecurity educated community. *IEEE Transact. Emerg. Top. Comp.* 10, 1456–1463. doi: 10.1109/TETC.2021.3093444

AJP-3.20 (2020). *Allied Joint Doctrine For Cyberspace Operations*. Nato Standardization Office (NSO). Available online at: https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320 (accessed January 20, 2023).

Andress, J., and Winterfeld, S. (2013). *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners, 2nd Edn*. Oxford: Syngress.

Atlantic Council (2021). *A Primer on the Proliferation of Offensive Cyber Capabilities*. Washington, DC: Atlantic Council.

Barber, D. E., Bobo, T. A., and Sturm, K. P. (2016). Cyberspace operations planning: operating a technical military. *Milit. Cyber Aff.* 1:6. doi: 10.5038/2378-0789.1.1.1003

Braun, V., and Clarke, V. (2006). Using thematic analysis in psychology. *Qual. Res. Psychol.*, 3, 77–101. doi: 10.1191/1478088706qp063oa

Conti, G., Weigand, M., Skoudis, E., Raymond, D., Cook, T., and Arnoldt, T., et al. (2014). Towards a cyber leader course modeled on Army Ranger School. *Small Wars J.* Available online at: https://smallwarsjournal.com/jrnl/art/towards-a-cyber-leader-course-modeled-on-army-ranger-school

Dekić, M. D. (2022). How to transfer cyber security skill. *Tehnika* 77, 399–402. doi: 10.5937/tehnika2203399D

Elia, G., and Margherita, A. (2022). A conceptual framework for the cognitive enterprise: pillars, maturity, value drivers. *Technol. Anal. Strat. Manag.* 34, 377–389. doi: 10.1080/09537325.2021.1901874

Flick, U. (2019). *From Intuition to Reflexive Construction: Research Design and Triangulation in Grounded Theory Research*. New York City, NY: SAGE Publications Ltd.

GAO (2022). *Cyber Command Needs to Develop Metrics to Assess Warfighting Capabilities*. Washington, DC: United States Government Accountability Office: View GAO-22-104695.

Gozdziewicz, W. (2019). *Cyber Defence Magazine*. Allies (SCEPVA). Available online at: https://www.cyberdefensemagazine.com/sovereign-cyber/ (accessed November 11, 2019).

Herrick, D., and Herr, T. (2016). *Combating Complexity: Offensive Cyber Capabilities and Integrated Warfighting*. Available online at: https://ssrn.com/abstract=2845709

Huskaj, G., and Axelsson, S. (2023). "A whole-of-society approach to organise for offensive cyberspace operations: the case of the smart state Sweden," in *Proceedings of the 22nd European Conference on Cyber Warfare and Security, ECCWS 2023* (Piraeus: Academic Conferences and Publishing International Ltd.), 592.

Joint Publication 1 (2023). *Joint Publication 1 Volume 1*. Doctrine for the Armed Forces of the United States. Available online at: https://keystone.ndu.edu/Portals/86/Joint%20Warfighting.pdf (accessed August 27, 2023).

Jones, R. M. (2015). "Modeling and integrating cognitive agents within the emerging cyber," in *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) 2015 (p. 2015 Paper No. #15232 Page 1 of 10)* (Arlington, VA). Available online at: https://www.iitsec.org/ (accessed June 14, 2019).

Jones, R. M. (2019). *Cognitive Agents for Adaptive Training in Cyber Operations. HCII 2019: Adaptive Instructional Systems*. Orlando, FL: Springer Nature Switzerland AG 2019, 505–520.

Jøsok, Ø., Lugo, R., Knox, B. J., Sütterlin, S., and Helkala, K. (2019). Self-regulation and cognitive agility in cyber operations. *Front. Psychol.* 10:875. doi: 10.3389/fpsyg.2019.00875

Khanna, P. (2019). "Cognitive education framework for cyber security: a collaborative community approach aligning to tenets of Ako," in *Proceedings of the 2019 Conference* (Hamilton).

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. Pittsburgh, PA: RAND Corporation.

McNeese, M. D., and Hall, D. L. (2017). *The Cognitive Sciences of Cyber-Security: A Framework for Advancing Socio-Cyber Systems. Theory and Models for Cyber Situation Awareness* (Frankfurt: Springer), 173–202. Available online at: https://www.springer.com/series/0558

NATO (2016). *The North Atlantic Treaty Organization*. Warsaw Summit Communiqué. Available online at: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (accessed July 09, 2019).

NATO (2018). *The North Atlantic Treaty Organization*. NATO Summit set to begin in Brussels. Available online at: https://www.nato.int/cps/en/natohq/news_156597.htm (accessed July 10, 2018).

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *Int. Secur.* 41, 44–71. doi: 10.1162/ISEC_a_00266

Selján, G. (2023). Assessing offensive cyber capabilities. *Acad. Appl. Res. Milit. Public Manag. Sci.* 22, 5–18. doi: 10.32565/aarms.2023.3.1

Smeets, M. (2018). Integrating offensive cyber capabilities: meaning, dilemmas, and assessment. *Defence Stud.* 18, 395–410. doi: 10.1080/14702436.2018.1508349

Smeets, M., and Lin, H. (2018). "Offensive cyber capabilities: To what ends?," in *2018 10th International Conference on Cyber Conflict (CyCon)* (Tallinn: IEEE), 55–72.

Tayeb, S., Raste, N., Pirouz, M., and Latifi, S. (2018). "A cognitive framework to secure smart cities," in *2018 3rd International Conference on Measurement Instrumentation and Electronics (ICMIE 2018)* (Las Vegas, NV: EDP Sciences), 6.

Tracy, S. J. (2010). Qualitative quality: eight "big-tent" criteria for excellent qualitative research. *Qual. Inq.* 16, 837–851. doi: 10.1177/1077800410383121

U.S. Department of Defense (2015). *The DoD Cyber Strategy*. Available online at: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (accessed September 18, 2018).

Walcott, T. (2015). Training cyber forces without warfighting. *J. Inf. Warfare* 14, 7–15. Available online at: https://www.jstor.org/stable/26487490

Weick, K. E. (2007). The generative properties of richness. *Acad. Manag. J.* 50, 14–19. doi: 10.5465/amj.2007.24160637

Appendix 5

Publication V

Arik, Marko; Ottis, Rain; Venables, Adrian; Lugo, Gregorio, Ricardo (2025). Enhancing Operational Planning and Situational Awareness for Cyberspace Operations. 24th European Conference on Cyber Warfare and Security.

Enhancing Operational Planning and Situational Awareness for Cyberspace Operations (CO), Based on the Crossed Swords Exercises

Marko Arik[1], Adrian Nicholas Venables[1], Rain Ottis[1] and Ricardo Gregorio Lugo[2]
[1]Department of Software Science, Tallinn University of Technology Estonia
[2]Department of Welfare, Østfold University College, Halden, Norway

marko.arik@taltech.ee
adrian.venables@taltech.ee
rain.ottis@taltech.ee
ricardo.g.lugo@taltech

Abstract: Cyberspace Operations (CO) planners face unique challenges in modern warfare, requiring a comprehensive understanding of cyberspace layers and a systematic planning framework. Exercises such as Locked Shields and Crossed Swords (XS) enhance cybersecurity skills, teamwork, and decision-making under pressure. Visual planning tools can improve operational planning and situational awareness in COs by providing a holistic picture of the operating environment. This facilitates better decision-making and coordination and fosters a cooperative defence mindset among allies. Using lessons from XS, this study uses a design science methodology to create a Cyber Planner application. The research team was able to observe current procedures, evaluate the efficacy of current tools, and get input from CO planners participating in the exercise. XS offered a valuable framework for identifying operational issues in cyber operations planning. Through iterative design modifications based on user experiences and needs, the exercise provided a real-world testing ground to assess the Cyber planners' initial version. The study intends to improve situational awareness and operational planning skills in cyberspace using the lessons acquired from the exercise. The user requirements for the Cyber Planning tool were identified through a literature review and interviews, resulting in 30 user requirements included in an online survey. The online survey, which was directed at CO planners, validated most of the identified user requirements, ensuring the tool meets the demands and expectations of its intended users. Integrating risk management into a CO planning tool can improve situational awareness, response times, and defence strategies, enabling real-time monitoring, analysis, and decision-making. Advanced data visualisation and Cyber planning tools are needed for improved decision-making.

Keywords: Cyberspace operations, Visualising cyber planning, Cyber planning tool, Situational awareness, User requirements

1. Introduction

CO planners face challenges in aligning traditional military planning frameworks with the dynamic and complex requirements of COs. CO planners must analyse the operational environment and develop Courses of Action that navigate technical peculiarities inherent to cyberspace (VanDriel, 2016). Effective planning for Defensive Cyber Operations (DCO) and Offensive Cyber Operations (OCO) requires a tailored approach that integrates CO-specific factors while aligning with the Military Decision-Making Process (MDMP). Visual planning tools play a pivotal role in CO by offering a cohesive view of the operational environment, facilitating the integration of both friendly and adversary assets, identifying vulnerabilities, evaluating risks, and supporting the development of effective strategies (Pullen, 2015). This research explores how visual planning tools can enhance operational planning and situational awareness (SA) in CO, focusing on applying standardised symbology and real-time data integration. The XS exercise series is a critical reference point for this study, as it explores NATO's current CO planning frameworks and highlights vital gaps in SA.

The main objective of this study is to propose enhancements to NATO's CO planning and SA tools. This includes developing a Cyber planner tool that improves the integration of cyber assets in the MDMP, supports standardised symbology, and enables real-time data visualisation. This paper aims to answer the main research question, which is divided into sub-questions to help clarify and find more detailed responses.

RQ1 *How can operational planning and SA for COs be enhanced?*

RQ2 *What essential layers are involved in planning COs, and how do they contribute to effective cyber mission execution?*

RQ3 *How can operational visualisation tools enhance cyber situational awareness (CSA) in COs?*

RQ4 *What are the user requirements for the COs Planning Tool?*

2. Methods

This paper uses design science methodology with Exercise XS for experimental research (Kosmol, 2019). It involves a literature review and structured interviews with subject matter experts to develop and identify the user requirements for a Cyber planner tool. The review will focus on conceptual frameworks supporting operational planning, SA, and visualisation. Framework analysis will assess their applicability and effectiveness, followed by expert feedback and an online survey to validate the Cyber planner tool`s user requirements.

The authors offer suggestions for enhancing SA and operational planning, mainly COs. To find valuable improvements for COs planning and decision-making procedures, the writers will examine the results of the XS exercise. This entails evaluating crucial components such as CSA and visualisation tools and creating frameworks to complete cyber missions successfully. Their research aims to match these enhancements with the requirements and difficulties brought to light by professional opinions and actual workout situations.

2.1 Methodology

This research utilised the Design Science Methodology (DSM) to enhance CO's operational planning and situational awareness (Kosmol, 2019). The process involved identifying gaps in current frameworks, defining objectives, designing a new conceptual framework, creating a conceptual model, evaluating it through expert feedback, surveys, and case studies, iteratively refining the model based on feedback, and finally documenting the process and findings. The DSM approach is widely recognised in information systems and technology research, focusing on designing and building artefacts that contribute to theory and practice. The process graphic in Figure 1 depicts the stages of the DSM applied to this research.

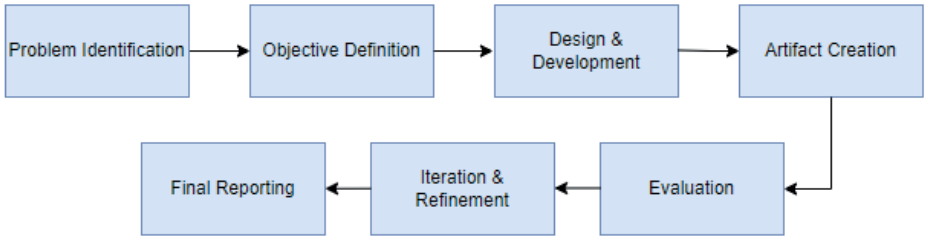

Figure 1: Design Science Methodology Process Flow

3. Literature Review

The literature review explores the potential of logical layer visualisation in improving SA and decision-making in CO planning, particularly in creating action plans. The research focuses on the importance of a multi-layered approach to cyberspace activities. It used keywords such as "Cyberspace Situation Awareness," "Visualising Cyberspace Operations," and "Visualisation of Cyberspace Operations" to define the investigation's scope. A systematic search was conducted using search phrases about CO planning, CO framework, and visualisation approaches. After a preliminary evaluation, 45 relevant papers were found, with 37 chosen for further examination. The literature used in the review is listed in Mapping of Literature Sources to Research Questions (M.Arik, 2025). The review focuses on cyberspace situation awareness and enhanced awareness through operational visualisation tools, focusing on cyberspace layers, the impact of visualisation tools, and user requirements for the Cyber Planner Tool. Visualisation techniques help represent complex data for better understanding and decision-making (Goethals & Hunt, 2019).

3.1 Cyberspace Situation Awareness

Situation awareness is the understanding and perception of environmental elements, meaning, and future projections, which are crucial for decision-making in military operations and industrial settings (Endsley, 1995).

CSA contributes to accurate risk and threat assessments, as highlighted by NATO (AJP-3.20, 2020). It involves dynamic information management, analysis, and a near real-time understanding of cyberspace (U.S. ARMY, 2013). Appreciating cybersecurity's characteristics, risks, threats, and security needs is essential for enhancing cybersecurity. A three-layer paradigm for understanding cyberspace has been introduced, focusing on SA, resilience, and counterattacks (Venables, 2021). This framework can be expanded to include human factors, geography, data routes, and security and examine how hostile actors' intentions affect risk mitigation.

Situation awareness is context-dependent and individualised, with the Cyber Forces Interactions Terrain version using three essential parts: knowledge of the current state, comprehension of that state, and projection of that state. The purpose of SA measures is not to gain a perfect understanding but rather a general understanding (Dobson & Carley, 2021).

As addressed by NIST, security awareness focuses on recognising and mitigating security risks and threats (NIST, 2014). Effective icon design is vital for rapid CSA, as it involves perceiving, understanding, and predicting threats to manage cyber threats effectively (Kookjin et.al, 2023). Both situational and security awareness are essential for informed decision-making and performance in military and industrial contexts, particularly in cyberspace.

3.2 Enhanced Cyber Situational Awareness Through Operational Visualisation Tools

Recent studies suggest that military commanders can improve CSA using operational picture principles (Army Techniques Publication, 2024; Pfannenstiel & Cox, 2024; Kookjin et.al, 2023; Llopis et al., 2018). Advanced visualisation tools, such as the Cyber Common Operational Picture (CyCOP) and the Royal Military Academy's 3D Operational Picture, enhance this awareness (Llopis et al., 2018). These tools use sophisticated concepts that help commanders understand the implications of cyber defence strategies. The study emphasises the importance of a comprehensive CSA system for military commanders, integrating pictures with risk assessments and mission planning. The Cyber Order of Battle approach is recommended for further validation. The U.S. Army is developing frameworks to visualise commanders' areas of operations in physical, cognitive, and virtual dimensions, enhancing understanding of cyberspace opportunities, risks, and vulnerabilities (U.S. ARMY, 2013).

Another study focuses on the Common Operational Picture (COP). This study finds that visualisation contributes to SA in cyber battle training, as it helps provide a detailed understanding of the Red and Blue Teams' cyber situation. A person using the data visualisation screen can quickly identify the scenario. In this case, the COP is a successful command and control system in the military (Kookjin et al., 2023).

Recognising the cyber situation using easily understandable symbols is necessary to rapidly prepare for and respond to a cyber-attack. Kookjin et al. proposed using Cyberspace Symbol Components from the MIL-STD-2525D (Department of Defense, 2014). The CyCOP visualisation screen uses a common standard to express cyberspace objects as hexagons with symbols or characters. MIL-STD-2525D proposes a versatile expression method utilising a frame, icon, and fill for graphic representation. This method can be used on accurate maps and cyberspace (Ibid).MIL-STD-2525D, a military symbology document, does not currently include cyberspace symbols for diverse entities and activities in COs. This provides network architecture, cyber threats, digital communication channels, and unique cyberspace-related elements for effective military planning and visualisation tools.

Cyber commanders and planners must understand COs to visualise end states and describe intent, especially in Offensive Cyber Operations (OCO) (Bender, 2013). The U.S. Army is developing frameworks to visualise commanders' areas of operations in physical, cognitive, and virtual dimensions, enhancing their understanding of cyberspace opportunities, risks, and vulnerabilities (U.S. ARMY, 2013). Combining knowledge and visualisation techniques ensures commanders can navigate complex operational environments and respond to emerging threats.

Additionally, Klipstein's research demonstrated the effectiveness of an OCO risk framework with graphical outputs in aiding personnel needing more necessary experience, suggesting that these graphics mitigate the need for national-level experience (Klipstein, 2019).

Monitoring information systems and utilising visualisation techniques are essential for effective security strategies and operational planning (Goethals & Hunt, 2019). Advanced technologies can help visualise and predict battlespace, enhancing understanding of operational and environmental complexities (Bryant, 2016).

Colours enhance SA in cyberspace, aiding decision-making and understanding complex cybersecurity concepts through visual representation in cyberspace training (Dobson & Carley, 2021) (NIST, 2014). The NIST 2017 framework emphasises the importance of visualisation tools and communication skills in various cybersecurity roles, enabling efficient decision-making and collaboration in cyber operations planning (NIST, 2017). Decision makers are more confident and precise when given more choices, and modern cybersecurity operations must adapt to the technology industry's design and visualisation, focusing on contextualising data rather than attempting to visualise all available information (Ward, 2023). OCO planners can effectively utilise visualisation

to aid decision-making, enhance SA, and achieve operational goals by focusing on contextualising data rather than presenting all available information.

Graphic control measures in land domains can be adapted for SA in cyberspace, using offensive, defensive, and tactical mission graphics to depict actions (McCroskey & Mock, 2017). Wang proposes a method for creating a cyberspace map model using IP addresses, but further development and testing are required for practical application (Wang et. al., 2021). Wong et al. propose a framework for CSA, integrating it into a cyber operation planning tool for real-time monitoring, analysis, and decision-making (Wong et. al., 2021). Gutzwiller`s study highlights the need for enhanced training and skill development in Cyber Operations situational analysis and the effectiveness of user-centred design in addressing specific population needs (Gutzwiller et al., 2016).

Governments' proprietary cyber operations tools like Argos software demonstrate advanced monitoring and defence capabilities. They visualise cyberspace for governments, businesses, and individuals and indicate significant offensive cyberspace capabilities (Innovation Development Institute, 2009). Another tool, the Cyberspace Effects Server, provides comprehensive cyberspace visualisations for mission planning and execution tasks, enhancing understanding of COs and kinetic domain tactics. Still, it requires further integration for enhanced effectiveness (Hasan et al., 2021).

3.3 Frameworks Guiding Cyberspace Operations

The operational framework is a cognitive tool that aids commanders in visualising and describing combat power applications, enhancing decision-making, communication, scenario planning, training, and SA (Army Techniques Publication, 2024). NATO's Allied Joint Doctrine for Cyberspace Operations guides joint operations planning and assessment, integrating voluntary cyber effects from allies into Alliance missions (AJP-3.20, 2020) (Goździewicz, 2019). COs significantly impact military operations, but cyber operational planning has not been fully addressed in the past decade. Clear objectives and historical analyses are needed for new CO strategies (VanDriel, 2016). COs necessitate understanding system posture, adaptation to adversaries, and data-driven operations to address dynamic assets, complex communication paths, and new attack surfaces (Ziring, 2015). A 2013 US Army white paper presents the LandCyber framework, a unified operational and institutional solution for Army COs from 2018-2030, focusing on unified COs and enhanced understanding (U.S. ARMY, 2013). The US military is exploring the Trilateral Strategic Initiative (TSI) to develop an agile operational assessment framework for IT, acquisition, and COs, enhancing interoperability and trust (Bryant, 2016).

Cyber-FIT Version 4 is a simulation framework for cyber team performance modelling, addressing contested environments' cyber mission forces. Agile software development processes such as Scrum and DevSecOps optimise cyber range planning, managing new technologies, vulnerabilities, and patches, and supporting CO plans (Dobson & Carley, 2021) (Carroll, 2023).

Over the past two decades, scientific research on DCOs has primarily focused on developing techniques, algorithms, and constructs to support active and passive efforts (Goethals & Hunt, 2019).

The NIST Special Publication aids in security control assessments and risk management, focusing on IT/cybersecurity personnel in Federal Organizations. It also includes the Cyber Operational Planner speciality area, enhancing cybersecurity personnel's understanding and mitigating risks within their organisations. Integrating cybersecurity principles, risk management, and operational requirements into training and planning processes enhances readiness for complexities (NIST, 2014) (NIST, 2017).

Sulin's study examines how non-state actors such as Anonymous used cyber-attack methods in their 2016 campaign and compares them to established frameworks. The canonical model of OCOs provides a comprehensive overview, but future research needs accurate frameworks, post-attack analysis, and larger-scale analysis (Sulin, O, 2018).

Klipstein's paper uses decision-maker preferences, risk analysis, and simulation modelling to aid commanders in OCOs, especially for inexperienced personnel. It offers practical insights, but more holistic frameworks are needed (Klipstein, 2019).

The study by Kookjin et.al. (2023) suggests that enhancing CSA through the Cyber Common Operational Picture Framework can aid military and private sector cyber defence training. It emphasises the importance of recognising cyberspace, addressing planning gaps, enhancing SA, focusing on operational-level improvements, and integrating cyberspace into planning processes.

The U.S. Army Techniques Publication offers a comprehensive approach to CO Planning, including cyberspace layers, terrain analysis, threat description tables, terrain effects matrix, event matrix, hybrid threat analysis, and hybrid threat analysis, ensuring effective COs and security for operational-level decision-making (Army Techniques Publication, 2024).

3.4 Integrating Situational Awareness in Cybersecurity Visualisations

Standard rules for symbol construction and generation are needed for joint military symbology. Ineffective communication between cyber and physical domain warriors hinders the practical application of operational campaign design and war principles in COs. Cyberspace operational graphics can help cyber planners and operators communicate mission-relevant information to warfighters unfamiliar with the technical details of cyberspace, potentially leading to the identification of parallels and analogies in the physical domain (McCroskey & Mock, 2017).

This study examines visualisation techniques for CSA in military contexts, focusing on operational-level staff. It highlights a gap in understanding stakeholders and information types in visualisations. It emphasises the importance of SA for timely decision-making and the need for more scientific research on CSA visualisations. It suggests designing CSA visualisations based on user needs and preferences, reducing complexity and allowing easy sharing (Jiang et al., 2022).

This paper discusses the need for more research on situation awareness in Security Operation Centres (SOCs), highlighting the need for more theoretical foundations and understanding of its impact on human operators' performance. It suggests further investigation and exploration of tools for operationalising SA (Ofte & Katsikas, 2023). Advanced visual tools should incorporate predictive analytics for real-time threat forecasting and vulnerability identification, enhancing decision-making capabilities, such as network maps, in detecting and managing cyber threats (Barford et.al., 2010). Franke and Brynielsson emphasise incorporating human factors into cybersecurity, advocating for real-time visualisation tools to provide contextual information about threat severity and potential impacts (Franke & Brynielsson, 2014). Renaud and Ophoff suggest that CSA tools should be user-friendly and practical, guiding users through security information interpretation and response strategies (Renaud & Ophoff, 2021).

The final paper in this review highlights the importance of human-to-human communication in cyber defence decision-making and identifies inefficiencies in security operations. It suggests that 3D mixed reality visualisation can enhance CSA without directly impacting decision-making processes, highlighting the need for further research (Ask et al., 2023).

This section explains the requirement to develop advanced visual tools and standardised symbology for command-and-control systems to bolster joint military operations. Such enhancements are essential for improving SA and facilitating more effective decision-making in CO.

3.5 User Requirements From the Literature Review for the Cyber Planner Tool

This subsection outlines the essential user requirements and compatibility features necessary for the effective deployment and operation of the Cyber Planner tool, as detailed in the literature review chapter.

The Cyber Planner tool is crucial for COs, enhancing commanders' understanding of cyberspace activities. It should interface with established frameworks like AJP-3.20, LandCyber, and NIST recommendations (AJP-3.20, 2020) (U.S. ARMY, 2013) (NIST, 2014). Advanced visualisation tools facilitate interoperability and offer decision assistance (McCroskey & Mock, 2017)(Klipstein, 2019) (Bryant, 2016). The tool should incorporate risk management frameworks, support DCOs, analyse political conflicts, and offer decision assistance (Wong et. al., 2021) (NIST, 2022). It should provide real-time information management, a comprehensive operational picture, context-dependent awareness, integration with security awareness principles, icon design, and threat behaviour analysis (AJP-3.20, 2020) (Venables, 2021) (Dobson & Carley, 2021) (Kookjin et.al, 2023) (NIST, 2014). It should also offer comprehensive visualisation capabilities, contextualised information representation, military symbology, 3D mixed reality visualisations, automated frameworks, and tailored training for cyber operations analysts and planners (Mohite, S, 2018) (Wong et. al., 2021) (Gutzwiller et. al., 2016) (Hasan et. al, 2021). The tool should also incorporate predictive analytics, dynamic data presentation, and human factors to make complex data comprehensible to operators in real time (Ask et al., 2023). It should be designed with practical and user-friendly features that align with the resource constraints of small and medium enterprises (Renaud & Ophoff, 2021). This review emphasises the need for standardised frameworks, improved CSA, sophisticated visualisation tools, and user-specific modifications for successful CO planning and execution.

The literature review identified key user requirements for a CO planning tool, including real-time threat monitoring, cyber terrain mapping, interoperability with military command structures, and decision-support mechanisms. Comparison of Tools and Frameworks for Cyber Operations Planning shows a table comparing the identified tools and frameworks for relevance (Arik, 2025).

4. Results of Interviews

Semi-structured interviews were conducted with XS 2021 Higher Command, Cyber Headquarters (CHQ) staff officers, and Tactical Commanders to gather contextual and nuanced information about operational, technical, and strategic subjects. Interviews were conducted with six cyber operations professionals with varying IT, cybersecurity, and military operations backgrounds. This sample represents a focused subset of cyber operators, though its representativeness relative to the total population remains an open question. The recruitment process involved selecting experienced professionals engaged in CO exercises, ensuring relevant insights into operational planning challenges. Inquiries were made about the participants' professional backgrounds, the XS 2021 exercise's planning methodology and particular user needs for a Cyberspace Operations Planning Tool. Their answers emphasised the need for more excellent data visualisation, better interaction with standard frameworks, more situational awareness, and gaps in the existing operational tools. After analysing the responses, the researcher found recurrent themes and demands incorporated into the survey for broader validation.

The study explored the CHQ planning process in the XS 2021 exercise and user requirements for the CO Planning tool through a methodical process including research objectives, literature review, expert consultation, and semi-structured interviews. The interviews focused on the interviewee's background, planning process, and tool requirements. The interviewees had IT, cybersecurity, military operations planning, and security architecture degrees. They had at least eight years of CO experience and planned CO exercises, and they are currently involved in higher-level planning, cybersecurity architecture research, and security operations centre management. The following summarises the proposed user requirements for the Cyber Planner Tool.

The CO Planning Tool should include layers for a comprehensive view of the cyber environment, filters for quick connections, and colourful, easy-to-understand symbols. The tool should display asset properties and information when the user moves their mouse over it and allow them to combine physical assets into logical layers. The tool should be user-friendly, using symbols like standard ICT tools, and integrate seamlessly with existing frameworks. It should also feature automatic application programming interfaces for mapping tactics to frameworks such as MITRE, robust filtering options, and grouped networks for easy viewing. MITRE ATT&CK® is a globally accessible knowledge base for adversary tactics and techniques used in private, government, and cybersecurity sectors for developing threat models and methodologies (MITRE, 2025).

Developing standard operating procedures (SOP) for COs can be challenging due to the divide between military and cyber backgrounds. A dual system can improve operational planning and streamline the process. The Cyber Planners tool should be a comprehensive management system integrating asset information and SA with configuration management database-like functionalities for inventory management and semi-automated updates. It should also incorporate filtering options for better management of network devices, information and communications technology assets, adversary units, and own units, as well as a geographical map for enhanced visualisation and operational capabilities.

Due to infantry-based approaches and technical details, the CHQ faces challenges developing SOPs. Staff procedures are insufficient for fast-paced COs; detailed task descriptions are needed for operations and planning cells. The Cyber Planners tool should be a comprehensive management system integrating asset information, SA, inventory management, and data exchange. It should also incorporate filtering options to manage network devices, ICT assets, adversary units, and own units better.

One interviewee needed a CO Planning Tool to analyse cyber and physical operational landscapes, including IT and risk management. The tool should identify vulnerabilities, align with forces' capabilities, and incorporate Allied Joint Doctrine joint functions. It should provide strategic-level information, assess risks, and catalogue critical assets. Universal symbols should be used to ensure understanding across command levels. The tool should enable real-time battle damage and operational assessments.

Another interviewee highlighted the challenges in the Cyber Command planning process due to the lack of integration and digitalisation. The process needed to be more cohesive and relaxed, requiring less time-consuming searches. She suggested a digital CO planning tool to streamline processes and enhance

operational efficiency. The proposed tool would address synchronisation issues in section briefings, ensure a clear understanding of operations, and improve timeliness. The Cyber Planners tool aims to enhance automation, integration, and real-time capabilities, reducing human error and improving efficiency. It should also facilitate report creation and coordination across tactical, operational, and strategic command levels.

A further Interviewee suggested a user-friendly COs Planning Tool with comprehensive information on adversaries' strategies and visual aids. The tool should integrate with platforms like MIPS, support precise targeting and planning, and be compatible with NATO planning systems. It should have strong filtering capabilities, automated reporting, and a chronological timeline.

The XS exercise highlighted the importance of a planning tool in the operations department. Operational processes can be improved, and standardised templates and better structuration are needed to enhance metadata management and data handling.

5. Proposed Enhancements for Operational Planning and Situational Awareness for COs

In XS 2020, the CHQ developed an operational plan for sub-units, focusing on the Military Decision-Making Process and improving procedures. However, the higher command realised the need to align the plan with the exercise timeline. The CHQ used open-source drawing tools for visual operational planning, allowing for SA and practical strategies to address cyber threats. In 2022, the CHQ adopted a new cyber exercise command structure and prepared the initial standard operating procedures.

By 2022, CHQ had evolved its cyber exercise command structure and introduced a preliminary version of standard operating procedures (SOPs). Additionally, it developed a Cyber Planner tool (Figures 2 and 3), introducing several enhancements:

- Advanced Filtering Options: The tool allowed planners to apply filters based on affiliation, targeting evaluation, targeting results, persona, and network devices.
- Enhanced Visualisation: New asset symbols with amplifiers improved clarity, while logical and dynamic asset connections provided a better operational overview.
- Targeting Assistance: The tool streamlined the targeting process, grouping Red Team units (considered Blue Team targets) in an organised layout (Figures 2 and 3).

Figure 2 provides a high-level view of the Cyber Planner tool, illustrating the operational environment used for cyberspace operations planning. The visual representation includes own forces, enemy assets, third-party elements, and cyber personas, each marked with distinct symbols and logical connections. The diagram highlights how planners interact with the tool to develop situational awareness and course-of-action (COA) strategies. Key features, such as dynamic linking of assets and real-time updates, support decision-making across strategic, operational, and tactical levels.

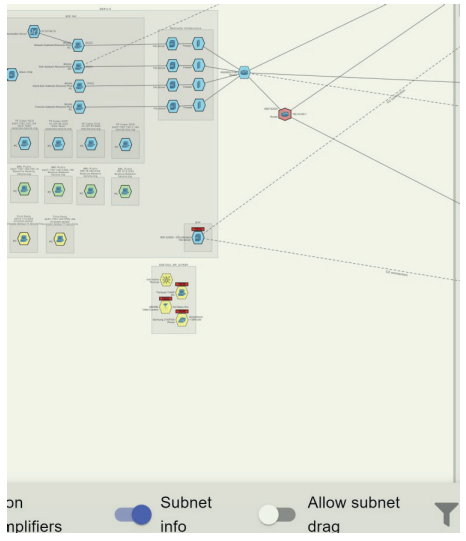

Figure 2: Proposed Cyber Planner tool with Blue team units

Figure 3 displays the Cyber Planner's user interface, explicitly showing Red Team units grouped as Blue Team targets. The left-side function menu includes various filtering options: affiliation, targeting evaluation, and network devices. The right-side control panel provides options to lock the screen, save the layout, and access settings. By zooming into key details, Figure 3 clearly depicts how planners interact with the system. These figures are an original contribution from the lead author, who created and modified the tool to optimise planning and execution procedures according to each team's unique requirements.

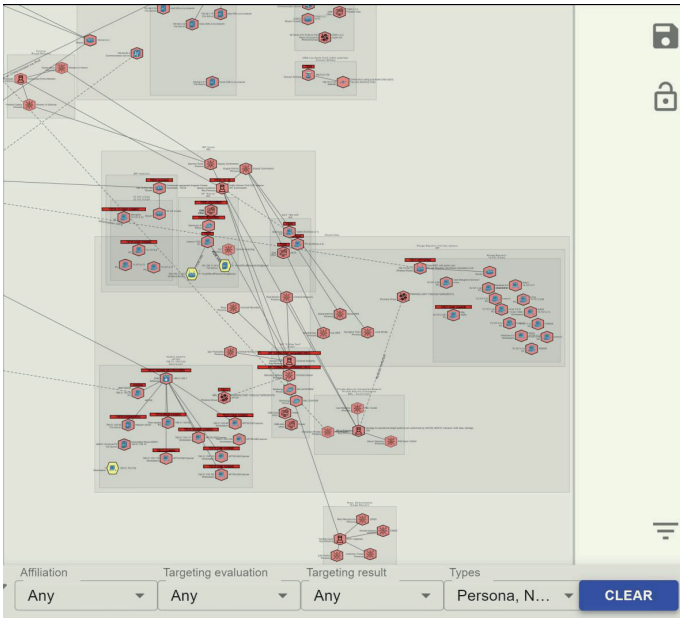

Figure: 3 Proposed Cyber Planner tool with Red team units

The tool assisted in identifying additional user requirements for future integration and acted as the first foundational test in CO planning. Even though it wasn't finished, it successfully illustrated how crucial logical connections, visual planning, filtering, and other aspects are to assisting with CO planning.

6. Results of Surveys

The survey validated 30 user requirements via Likert-scale responses from 22 cyber operations experts. A 70% agreement threshold confirmed most criteria for improving situational awareness and operational planning. Future validation is needed for real-time information management, human factors, API integration, and backend synchronisation. The dataset contains survey responses on cyber operations visual planning tools, with categorical responses. The histogram is presented in Figure 4.

The survey was completed by 22 participants from the NATO Cooperative Cyber Defence Centre of Excellence Integrating Cyberspace Considerations into Operational Planning Course. The survey's design, targeting specialised professionals from many nations, contributes to the findings' validity within the expert community. The identified and validated user requirements, their sources, and newly discovered ones are summarised in "User Requirements Validation for Enhancing Operational Planning and Situational Awareness in Cyberspace Operations" (Arik, Google Drive, 2025).

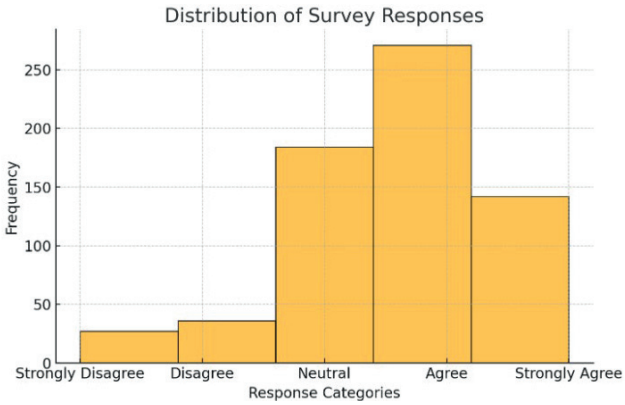

Figure 4: Distribution of Survey Responses on Cyber Operations Visual Planning Tool Features

7. Limitations and Future Work

The study's limitations include the interviewees being cybersecurity and military SMEs with at least eight years of experience in CO exercises and planning. The survey revealed four unvalidated user requirements, potentially compromising usability and efficiency. The 22-person sample size may be small for broad statistical generalisation but is strong in domains like COs. Future work will involve developing a CO visual planning tool and detailed planning processes.

8. Conclusions

The study effectively addressed the research questions by integrating findings from a literature review, expert interviews, and survey responses. It identified the logical, cyber-persona, and physical layers as essential to cyberspace operations. It demonstrated how their integration into a Cyber Planning Tool enhances operational planning and execution at multiple levels. Survey results confirmed that real-time operational visualisation tools improve CSA by providing explicit depictions of cyber assets and evolving threats, aiding decision-making. Additionally, 30 user requirements—validated by subject matter experts with over 70% agreement—highlighted the need for enhanced interoperability, automated asset tracking, and dynamic visualisation capabilities. These findings substantiate the necessity of advanced cyber planning tools for NATO and allied forces, confirming the study's conclusions with empirical evidence.

References

AJP-3.20. (2020, January). *ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS.* https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320

Army Techniques Publication. (2024, January 23). ATP 2-01.3, Intelligence Preparation of the Battlefield,Change No. 2,No. 2-01.3. Washington, DC, U.S.

Ask et al. (2023). A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness. *Sec. Cybersecurity and Privacy*, Online Volume 6 - 2023 | https://doi.org/10.3389/fdata.2023.1042783.

Barford et.al. (2010). Cyber SA: Situational Awareness for Cyber Defense. *In Cyber Situational Awareness*, 3-14.

Bender, J. M. (2013). The Cyberspace Operations Planner. *Small Wars Journal*.

Bryant. (2016). Mission Assurance through Integrated Cyber Defense. *Air and Space Power Journal*, 5-18.

Carroll, J. (2023). Agile Methods For Improved Cyber Operations Planning. *Proceedings of the 22nd European Conference on Cyber Warfare and Security, ECCWS 2023* (pp. 108-115).

Department of Defense. (2014, June 10). *JOINT MILITARY SYMBOLOGY.* http://everyspec.com/MIL-STD/MIL-STD-2000-2999/MIL-STD-2525D_50933/

Dobson, & Carley. (2021). *Cyber-FIT Agent-Based Simulation Framework Version 4.* Pittsburgh,: Center for the Computational Analysis of Social and Organizational Systems.

Endsley. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *The Journal of the Human Factors and Ergonomics Society, 37(1),*, 32–64.

Franke, & Brynielsson. (2014). Cyber situational awareness—A systematic review of the literature. *Computers & Security, 46*, 18-31.

Goethals & Hunt. (2019). A review of scientific research in defensive cyberspace operation tools and technologies. *Journal of Cyber Security Technology*, 1-48.

Goździewicz, W. (2019, November 11). *Cyber Defence Magazine*. Retrieved from Voluntarily by Allies (SCEPVA): https://www.cyberdefensemagazine.com/sovereign-cyber/

Gutzwiller et. al. (2016). A Task Analysis toward Characterizing Cyber-Cognitive Situation Awareness (CCSA) in Cyber Defense Analysts. *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, 14-20.

Hasan et. al. (2021). A Cyberspace Effects Server for LVC&G Training Systems. *2021 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC)* (pp. 1-12).

Innovation Development Institute. (2009). *Argos - Visualization Tool for Cyberspace Command and Control*. https://www.inknowvation.com/sbir/awards/af-2009-argos-visualization-tool-cyberspace-command-and-control

Jiang et al. (2022). Systematic Literature Review on Cyber Situational Awareness Visualizations. *IEEE Access, vol. 10*, 57525-57554.

Klipstein, M. (2019). Seeing is Believing: Quantifying. *THE CYBER DEFENSE REVIEW*, 88.

Kookjin et.al. (2023). Study on Cyber Common Operational Picture Framework for Cyber Situational Awareness. *Applied Sciences*, https://doi.org/10.3390/app13042331.

Kosmol, L. &. (2019). *ICT Usage in Industrial Symbiosis: Problem Identification and Study Design*. https://annals-csis.org/proceedings/2019/drp/pdf/323.pdf

Llopis et al. (2018). A comparative analysis of visualisation techniques to achieve cyber situational awareness in the military. *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, 1-7.

M.Arik. (2025, Jan 15). *Google Drive*. Mapping of Literature Sources to Research Questions: https://shorturl.at/nUd9g

McCroskey, & Mock. (2017). Operational Graphics for Cyberspace. *Joint Force Quarterly 85*, 43.

MITRE. (2025, Jan 15). *ATT&CK*. Retrieved from MITRE: https://attack.mitre.org/

Mock, & McCroskey. (2017, April 1). Operational Graphics for. *Joint Force Quarterly 85*, pp. Online [https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1130660/operational-graphics-for-cyberspace/].

Mohite, S. (2018, January 26). *Cybersecurity operations and the role of visualization, design, and usability.* Retrieved September 20, 2023, from https://medium.com/uplevel/how-design-visualization-and-usability-impact-cybersecurity-operations-61d854b5e2d3

NIST . (2022, May). *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

NIST. (2014). *A Role-Based Model for Federal Information Technology/Cybersecurity Training.* Virginia: U.S. Department of Commerce.

NIST. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* Gaithersburg,: U.S. Department of Commerce.

Ofte, & Katsikas. (2023). Understanding cyber situational awareness in SOCs. *Journal of Information Security and Applications, 62*, 102952.

Pfannenstiel, M., & Cox, D. (2024). NATO's Cyber Era (1999–2024) Implications for Multidomain . *MILITARY REVIEW ONLINE EXCLUSIVE · OCTOBER 2024*, 1-10.

Pullen, J. M. (2015). Visual planning for cyber operations. In M. O'Leary, *Cyber Operations: Building, Defending, and Attacking Modern Computer Networks* (pp. 221-239). Towson: Apress.

Renaud, & Ophoff. (2021). An SME-specific cyber situational awareness model to predict the implementation of cybersecurity practices. *Journal of Cybersecurity*, 24-46.

Sulin, O. (2018, FEB 16). CYBER ATTACK CAMPAIGNS IN POLITICAL CONFLICTS. Turku, Finland. https://www.utupub.fi/handle/10024/145536

U.S. ARMY. (2013). *THE U.S. ARMY LANDCYBER WHITE PAPER 2018-2030.* Fort George G. Meade,: U.S. Army Capabilites Integration Center.

VanDriel, M. (2016). Bridging the Planning Gap: Incorporating Cyberspace Into Operational Planning. *The Cyber Loop*, Online [http://thecyberloop.com/journal-article/].

Venables, A. (2021, November 16). *Frontiers in Education*. Retrieved from Modelling Cyberspace to Determine Cybersecurity Training Requirements: https://www.frontiersin.org/articles/10.3389/feduc.2021.768037/full

Wang et. al. (2021). *CYBERSPACE MAP MODEL CREATION METHOD AND DEVICE.* Houston: Patent Application Publication.

Ward, P. (2023). Choice, Uncertainty, and Decision Superiority: Is Less AI-Enabled Decision Support More? *IEEE TRANSACTIONS ON HUMAN-MACHINE SYSTEMS, VOL. 53, NO. 4, AUGUST 2023*, 781-791.

Wong et. al. (2021). A Framework for Measuring Situation Awareness in Cyberspace Operations. *Proceedings of the Human Factors and Ergonomics Society Annual MeetingVolume 65, Issue 1*, 358-362.

Ziring, N. (2015). The Future of Cyber Operations and Defense. *Journal of Information Warfare*, 1-5.

Appendix 6

Publication VI

Arik, Marko; How Do NATO Members Define Cyber Operations? (2023). HCI International 2023 – Late Breaking Posters. (8−14). SpringerLink. (Communications in Computer and Information Science; 1957).

How Do NATO Members Define Cyber Operations?

Marko Arik(✉)

Tallinn University of Technology, Tallinn, Estonia
marko.arik@taltech.ee

Abstract. This paper presents a systematic mapping study of NATO member states prominent in the cyber domain, and their interpretation of cyber terminology. NATO nations currently participate in a range of cyber exercises, but there is no unified conceptual framework for accepted cyberspace definitions to ensure interoperability. There is therefore a requirement for a common understanding of how member states define cyber operations.

This study seeks to determine if the doctrinal publications of NATO member states can answer the research question - How do NATO members define cyber operations?

The Systematic Mapping Study aims to provide a broad overview of the research area to provide evidence on the topic and its quantity.

60 national doctrinal publications were reviewed from 12 prominent NATO nations. Of these, ten defined cyber operations in a similar manner providing coherency in understanding the concepts involved. This provides a basis for successful cyber operations and exercises.

Keywords: NATO cyber operations definitions · Systematic Mapping Study · Literature Review

1 Introduction

The conceptual development of national cyberspace operations has evolved with the introduction of new technologies and techniques to exploit their capabilities. To a large extent, definitions and doctrines have reflected how individual states have embraced this new environment leading to a broad spectrum of different terminologies. NATO's recognition of cyberspace as a domain of operations in 2016 has led to the need for a common understanding of how it's members will engage in this new environment. This requirement has been accelerated by a growing interest in offensive cyber operations (OCO), which is expressed by the creation of cyber commands, branches, or services within their armed forces [2]. Training and exercising are conducted by the NATO-affiliated Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, which hosts the annual Exercise Crossed Swords[1]. Crossed Swords is an annual technical red teaming cyber

[1] https://ccdcoe.org/exercises/crossed-swords/

C. Stephanidis et al. (Eds.): HCII 2023, CCIS 1957, pp. 8–14, 2024.
https://doi.org/10.1007/978-3-031-49212-9_2

exercise training penetration tester, digital forensics experts and situational awareness experts. Crossed Swords has evolved from a straightforward technical training workshop to an exercise involving leadership training for the command element, legal aspects, and joint cyber-kinetic operations [3]. This exercise brings together participants from over 21 countries, including NATO and non-NATO member states, which jointly plan and carry out a range of offensive cyber activities. In planning and executing cyberspace operations, it is especially important that human-computer interactions begin communication with commonly understood concepts.

This article gives an overview of the range of definitions and types of cyber operations used among NATO's prominent cyber countries.

The reviewed doctrinal[2] publications of NATO member states provide an overview of how each nation defines their cyber operations by mapping their cyber operations terminology. Since 2016 NATO Joint Publications have released a series of publications on cyber operations and terminology. These are meant for NATO member states and form the basis for combined cyber operations. This review is focused on identifying if NATO member states follow this established doctrine. If it is not so, it then examines how their cyber operations terminology is defined.

2 Methods

A Systematic Mapping Study was conducted during this research following the steps of Guidelines for performing Systematic Literature Reviews in Software Engineering by Barbara Kitchenham [4]. These comprise the following 7 stages:

1) Identify the scope of research.
2) Formulate the research questions of the review.
3) Carry out mapping of the doctrinal cyber publications of selected NATO member states.
4) Analyse the data needed to answer the research question.
5) Extract data from the chosen doctrinal publications.
6) Summarise and analyse the study results.
7) Prepare a report on the results.

2.1 Scope of the Research

NATO has 31 [4] member states, and the doctrinal publications of the most prominent cyber countries were analysed in this Systematic Mapping Study. The choice of nations that were selected was based on the National Cyber Power Index 2020 [5]. These were the United States, United Kingdom, Netherlands, France, Germany, Canada, Spain, Sweden, Estonia, Turkey, Lithuania, and Italy. Although these were identified as the NATO nations with the greatest involvement in cyber operations, it should be noted that not all NATO members possess cyber capabilities. This further influenced the choice of national publications that were examined. This study was limited to publicly available sources and no nationally classified material was included.

[2] Doctrinal publications are considered as governmental, official publications concerning doctrines.

2.2 Validation

To determine the validity of the doctrinal publications of the selected NATO member states, national representatives were consulted. This was to determine whether their doctrinal publications needed to be more comprehensive and to verify the currency of the sources. For example, two national representatives Italy working at the NATO CCDCOE were interviewed who confirmed the validity of the of the sources identified. Conversely, the accuracy of the Spanish cyber definitions was determined to be inadequate due to inconclusive literature and the national representative being unable to provide confirmation of the currency of the publications.

3 Results

The doctrinal publications of the selected NATO member states were analysed with Fig. 1 indicating the distribution of the publications and whether cyber operations were defined.

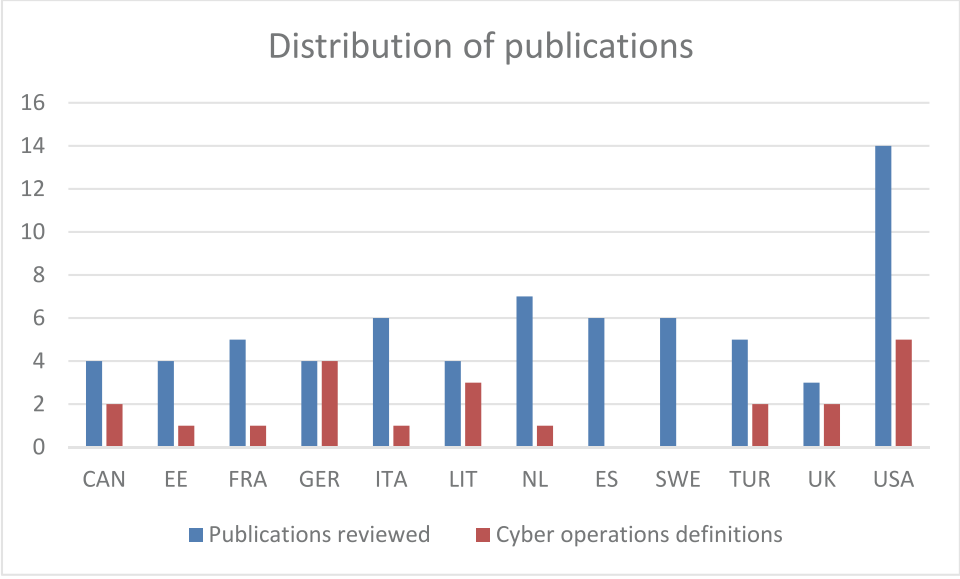

Fig. 1. Distribution of NATO cyber operations doctrinal publications

3.1 Temporal View of Publications

The year of publication of the national doctrinal publications that were examined is presented in Table 1 REF _Ref138149000 \h * MERGEFORMAT Publication date of NATO cyber operations doctrinal publications. The majority of the publications (15) were published in 2018, which relates to ~26% of the 56 publications. This was followed by 2020, when 11 publications were published, which formed ~ 19% of the total. No trend was identified from the data of publication date.

Table 1. Publication date of NATO cyber operations doctrinal publications

Year	CAN	EE	FRA	GER	ITA	LIT	NL	ES	SWE	TUR	GB	USA
2013					1							
2014						1						
2015					1	1						1
2016				1				1	1	1	2	1
2017		1	2		1	1		1				1
2018	1	1	1			1	2			1	1	2
2019	2	2			1		2	1				1
2020	2				1		1	3	1	1		2
2021	1		1	1	1							1
2022		1		1	1		1				1	
2023												1

3.2 Data Sources

Three main agencies were identified as the authors of the doctrine used by NATO nations These are presented in Table 2 Data source of NATO cyber operations doctrinal publications by the following sources: GOV - National governmental publication, MIL – Armed Forces publication and CCDCOE – The NATO CCDCOE publications.

Table 2. Data source of NATO cyber operations doctrinal publications

	Data sources		
	GOV	MIL	CCDCOE
CAN	6	-	-
EE	5	-	-
FRA	5	-	-
GER	1	1	1
ITA	6	-	1
LIT	3	-	1
NL	6	-	-
ES	5	-	1
SWE	1	1	-
TUR	2	-	1
UK	4	-	-
USA	8	2	-

The results of this research are shown in Table 3 Results, which indicates how prominent NATO member states define and classify their cyber operations. These are divided into defensive, offensive and intelligence cyber operations with the US having an additional category of Department of Defense Information Networks (DODIN).

Table 3. Results

	Defensive	Offensive	Intelligence Operations	Cybersecurity	DODIN
CAN		X		X	
EE	X	X		X	
FRA	X	X	X	X	
GER	X	X		X	
ITA	X	X	X	X	
LIT				X	
NL	X	X	X	X	
ES	X	X	X	X	
SWE	X	X	X	X	
TUR	X	X		X	
UK	X	X	X	X	
USA	X	X	X	X	X

4 Analysis

This article utilised an effective methodology to analyse selected NATO states' doctrinal publications to determine how they define cyber operations. Ten out of twelve states recognise and define defensive cyberspace operations. Eleven out of twelve recognise and define offensive cyberspace operations. In addition, seven out of twelve recognise intelligence operations in cyberspace. All the member states recognise cybersecurity. Exclusively, the United States has its Department of Defense Information Networks (DODIN) operations. The DODIN operations can be considered as a key terrain for the U.S. cyberspace. Key terrain in cyberspace is analogous to key terrain in a physical domain, in that access to or control of it affords any combatant a position of marked advantage [6].

From these results, it can be seen that these nations define their cyberspace operations to align with their own unique national cyber capabilities and requirements.

Furthermore, it can be seen that there is no agreed format or procedure on publishing and updating the cyberspace definitions across member states. The definitions are published according to individual timescales and are not related to each other. It was also found that the publications were not always easy to identify, and some were out of date

with regards to current NATO doctrine. This work identified a widespread weakness regarding the common understating of the cyberspace operations.

Overall, the study showed that allied member states have their own unique cyberspace definitions. This can lead to one member state understanding key aspects the cyberspace and its operations significantly differently from other member states.

5 Discussions and Conclusions

From this short investigation it can be concluded that there is a need for a single institution to maintain a common database of cyberspace terminology for NATO member nations. This central body should ensure that NATO member states align their cyberspace definitions and that they are recorded in an up-to-date database.

NATO's understanding of cyberspace activities needs to be clear and unambiguous to avoid issues from national publications being written in different languages to avoid issues with translation.

Scope of Cyber operations of the member states fulfils defensive, offensive or intelligence purposes with the United States adding a unique DODIN category. All of the nation's recognise cybersecurity. From most doctrinal publications, the essence of cyber operations could be identified, but not the degree of detail that can provide a comparable definition.

In order to establish common cyberspace activities and corresponding terms it is recommended that member states collaborate more to adopt common definitions.

NATO collaborative cyber defence and offensive exercises are increasing in complexity and sophistication. A common understating of cyberspace activities and their specific definitions is key to the success of these events and ensuring that operators from different nations can successfully work together.

Finally, a future study is proposed to investigate semantics and human-computer interaction in cyberspace doctrinal terms. [7].

Acknowledgments. Dr Adrian Nicholas Venables and Dr Rain Ottis from Taltech University.

References

1. Arik, M., Venables, A., Ottis, R.: Planning cyberspace operations: exercise crossed swords case study. J. Inf. Warfare **21**, 74 (2022)
2. CCDCOE, "Crossed Swords," The NATO Cooperative Cyber Defence Centre of Excellence (2023). [Online]. https://ccdcoe.org/exercises/crossed-swords/. Accessed 15 June 2023
3. Kitchenham, B.: Guidelines for performing systematic literature reviews in software engineering. IEEE Softw. Newcastle (2007)
4. NATO, NATO member countries (2023). https://www.nato.int/cps/en/natohq/topics_52044.htm. Accessed 21 June 2023
5. Belfer Center for Science and International Affairs John F. Kennedy School of Government, "National Cyber Power Index 2020 (2020). https://www.belfercenter.org/publication/national-cyber-power-index-2020. Accessed 15 June 2023

6. U.S. Air Force, “Air Force Doctrine Publication 3–12 - Cyberspace Operations,” (2023). https://www.doctrine.af.mil/Doctrine-Publications/AFDP-3-12-Cyberspace-Ops/
7. I. H. D. C. Julia Voo, “National Cyber Power Index 2022,” Belfer Center, Cambridge (2022)
8. K. A. L. Kaska Julgeolekuasutuste roll küberjulgeoleku tagamisel ja seda mõjutavad suundumused rahvusvahelises õiguses 2020. https://juridica.ee/article.php?uri=2020_2_julgeolekuasutuste_roll_k_berjulgeoleku_tagamisel_ja_seda_m_jutavad_suundumused_rahvusvahelis
9. Andrew, E.O.: HUMAN COMPUTER SYMBIOSIS (2016). https://arxiv.org/pdf/1601.04066.pdf. Accessed 21 June 2023

Curriculum vitae

Personal data

Name:	Marko Arik
Date of birth:	1982.04.26
Place of birth:	Tallinn, Estonia
Citizenship:	Estonian

Contact data

E-mail:	marko.arik@taltech.ee

Education

2021–2025	Tallinn University of Technology, Information Technologies PhD student
2011–2013	Tallinn University - Information technology management
2003–2005	Estonian Entrepreneurship University of Applied Sciences (EUAS) – Information technology (Applied higher education)
1998–2000	Tallinn Laagna Gymnasium

Language competence

Estonian	native speaker
English	fluent (B2 level)
German	basic (B1 level)
Finnish	basic (A2 level)
Russian	basic (A2 level)

Professional employment

2025–	Enefit Power OÜ
2021–2024	Talgen Cybersecurity OÜ
2001–2021	Estonian Defence Forces

Elulookirjeldus

Isikuandmed

Nimi:	Marko Arik
Sünniaeg:	1982.04.26
Sünnikoht:	Tallinn, Eesti
Kodakondsus:	Eestlane

Kontaktandmed

E-post:	marko.arik@taltech.ee

Hariduskäik

2021–2025	Tallinna Tehnikaülikool, infotehnoloogia doktorant
2011–2013	MBA, Tallinna Ülikool - Infotehnoloogia juhtimine
2003–2005	Eesti ettevõtluskõrgkool Mainor – Infotehnoloogia, rakenduskõrgharidus.
1998–2000	Keskharidus, Tallinna Laagna Gümnaasium

Keelteoskus

Eesti keel	emakeel
Inglise keel	kõrgtase
Saksa keel	algtase
Soome keel	algtase
Vene keel	algtase

Teenistuskäik

2025–	Enefit Power OÜ
2021–2024	Talgen Cybersecurity OÜ
2001– 2021	Eesti Kaitsevägi

ISSN 2585-6901 (PDF)
ISBN 978-9916-80-434-6 (PDF)