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)