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