Enhancing Operational Planning and Situational Awareness for Cyberspace Operations (CO), Based on the Crossed Swords Exercises

Marko Arik[1], Adrian Nicholas Venables[1], Rain Ottis[1] and Ricardo Gregorio Lugo[2]
[1]Department of Software Science, Tallinn University of Technology Estonia
[2]Department of Welfare, Østfold University College, Halden, Norway

marko.arik@taltech.ee
adrian.venables@taltech.ee
rain.ottis@taltech.ee
ricardo.g.lugo@taltech

Abstract: Cyberspace Operations (CO) planners face unique challenges in modern warfare, requiring a comprehensive understanding of cyberspace layers and a systematic planning framework. Exercises such as Locked Shields and Crossed Swords (XS) enhance cybersecurity skills, teamwork, and decision-making under pressure. Visual planning tools can improve operational planning and situational awareness in COs by providing a holistic picture of the operating environment. This facilitates better decision-making and coordination and fosters a cooperative defence mindset among allies. Using lessons from XS, this study uses a design science methodology to create a Cyber Planner application. The research team was able to observe current procedures, evaluate the efficacy of current tools, and get input from CO planners participating in the exercise. XS offered a valuable framework for identifying operational issues in cyber operations planning. Through iterative design modifications based on user experiences and needs, the exercise provided a real-world testing ground to assess the Cyber planners' initial version. The study intends to improve situational awareness and operational planning skills in cyberspace using the lessons acquired from the exercise. The user requirements for the Cyber Planning tool were identified through a literature review and interviews, resulting in 30 user requirements included in an online survey. The online survey, which was directed at CO planners, validated most of the identified user requirements, ensuring the tool meets the demands and expectations of its intended users. Integrating risk management into a CO planning tool can improve situational awareness, response times, and defence strategies, enabling real-time monitoring, analysis, and decision-making. Advanced data visualisation and Cyber planning tools are needed for improved decision-making.

Keywords: Cyberspace operations, Visualising cyber planning, Cyber planning tool, Situational awareness, User requirements

1. Introduction

CO planners face challenges in aligning traditional military planning frameworks with the dynamic and complex requirements of COs. CO planners must analyse the operational environment and develop Courses of Action that navigate technical peculiarities inherent to cyberspace (VanDriel, 2016). Effective planning for Defensive Cyber Operations (DCO) and Offensive Cyber Operations (OCO) requires a tailored approach that integrates CO-specific factors while aligning with the Military Decision-Making Process (MDMP). Visual planning tools play a pivotal role in CO by offering a cohesive view of the operational environment, facilitating the integration of both friendly and adversary assets, identifying vulnerabilities, evaluating risks, and supporting the development of effective strategies (Pullen, 2015). This research explores how visual planning tools can enhance operational planning and situational awareness (SA) in CO, focusing on applying standardised symbology and real-time data integration. The XS exercise series is a critical reference point for this study, as it explores NATO's current CO planning frameworks and highlights vital gaps in SA.

The main objective of this study is to propose enhancements to NATO's CO planning and SA tools. This includes developing a Cyber planner tool that improves the integration of cyber assets in the MDMP, supports standardised symbology, and enables real-time data visualisation. This paper aims to answer the main research question, which is divided into sub-questions to help clarify and find more detailed responses.

RQ1 *How can operational planning and SA for COs be enhanced?*

RQ2 *What essential layers are involved in planning COs, and how do they contribute to effective cyber mission execution?*

RQ3 *How can operational visualisation tools enhance cyber situational awareness (CSA) in COs?*

RQ4 *What are the user requirements for the COs Planning Tool?*

2. Methods

This paper uses design science methodology with Exercise XS for experimental research (Kosmol, 2019). It involves a literature review and structured interviews with subject matter experts to develop and identify the user requirements for a Cyber planner tool. The review will focus on conceptual frameworks supporting operational planning, SA, and visualisation. Framework analysis will assess their applicability and effectiveness, followed by expert feedback and an online survey to validate the Cyber planner tool`s user requirements.

The authors offer suggestions for enhancing SA and operational planning, mainly COs. To find valuable improvements for COs planning and decision-making procedures, the writers will examine the results of the XS exercise. This entails evaluating crucial components such as CSA and visualisation tools and creating frameworks to complete cyber missions successfully. Their research aims to match these enhancements with the requirements and difficulties brought to light by professional opinions and actual workout situations.

2.1 Methodology

This research utilised the Design Science Methodology (DSM) to enhance CO's operational planning and situational awareness (Kosmol, 2019). The process involved identifying gaps in current frameworks, defining objectives, designing a new conceptual framework, creating a conceptual model, evaluating it through expert feedback, surveys, and case studies, iteratively refining the model based on feedback, and finally documenting the process and findings. The DSM approach is widely recognised in information systems and technology research, focusing on designing and building artefacts that contribute to theory and practice. The process graphic in Figure 1 depicts the stages of the DSM applied to this research.

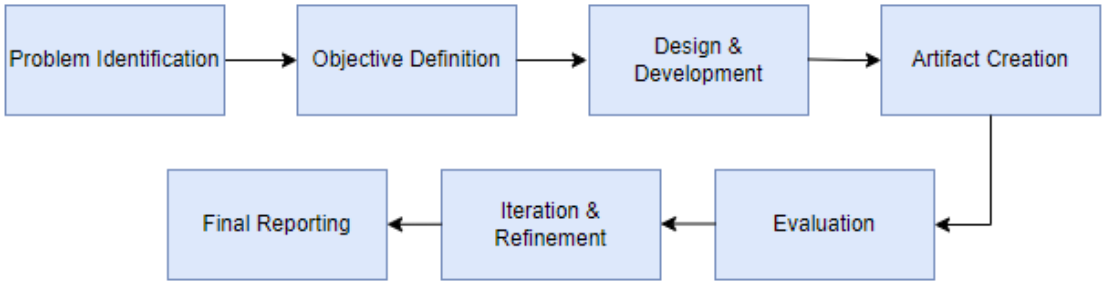

Figure 1: Design Science Methodology Process Flow

3. Literature Review

The literature review explores the potential of logical layer visualisation in improving SA and decision-making in CO planning, particularly in creating action plans. The research focuses on the importance of a multi-layered approach to cyberspace activities. It used keywords such as "Cyberspace Situation Awareness," "Visualising Cyberspace Operations," and "Visualisation of Cyberspace Operations" to define the investigation's scope. A systematic search was conducted using search phrases about CO planning, CO framework, and visualisation approaches. After a preliminary evaluation, 45 relevant papers were found, with 37 chosen for further examination. The literature used in the review is listed in Mapping of Literature Sources to Research Questions (M.Arik, 2025). The review focuses on cyberspace situation awareness and enhanced awareness through operational visualisation tools, focusing on cyberspace layers, the impact of visualisation tools, and user requirements for the Cyber Planner Tool. Visualisation techniques help represent complex data for better understanding and decision-making (Goethals & Hunt, 2019).

3.1 Cyberspace Situation Awareness

Situation awareness is the understanding and perception of environmental elements, meaning, and future projections, which are crucial for decision-making in military operations and industrial settings (Endsley, 1995).

CSA contributes to accurate risk and threat assessments, as highlighted by NATO (AJP-3.20, 2020). It involves dynamic information management, analysis, and a near real-time understanding of cyberspace (U.S. ARMY, 2013). Appreciating cybersecurity's characteristics, risks, threats, and security needs is essential for enhancing cybersecurity. A three-layer paradigm for understanding cyberspace has been introduced, focusing on SA, resilience, and counterattacks (Venables, 2021). This framework can be expanded to include human factors, geography, data routes, and security and examine how hostile actors' intentions affect risk mitigation.

Situation awareness is context-dependent and individualised, with the Cyber Forces Interactions Terrain version using three essential parts: knowledge of the current state, comprehension of that state, and projection of that state. The purpose of SA measures is not to gain a perfect understanding but rather a general understanding (Dobson & Carley, 2021).

As addressed by NIST, security awareness focuses on recognising and mitigating security risks and threats (NIST, 2014). Effective icon design is vital for rapid CSA, as it involves perceiving, understanding, and predicting threats to manage cyber threats effectively (Kookjin et.al, 2023). Both situational and security awareness are essential for informed decision-making and performance in military and industrial contexts, particularly in cyberspace.

3.2 Enhanced Cyber Situational Awareness Through Operational Visualisation Tools

Recent studies suggest that military commanders can improve CSA using operational picture principles (Army Techniques Publication, 2024; Pfannenstiel & Cox, 2024; Kookjin et.al, 2023; Llopis et al., 2018). Advanced visualisation tools, such as the Cyber Common Operational Picture (CyCOP) and the Royal Military Academy's 3D Operational Picture, enhance this awareness (Llopis et al., 2018). These tools use sophisticated concepts that help commanders understand the implications of cyber defence strategies. The study emphasises the importance of a comprehensive CSA system for military commanders, integrating pictures with risk assessments and mission planning. The Cyber Order of Battle approach is recommended for further validation. The U.S. Army is developing frameworks to visualise commanders' areas of operations in physical, cognitive, and virtual dimensions, enhancing understanding of cyberspace opportunities, risks, and vulnerabilities (U.S. ARMY, 2013).

Another study focuses on the Common Operational Picture (COP). This study finds that visualisation contributes to SA in cyber battle training, as it helps provide a detailed understanding of the Red and Blue Teams' cyber situation. A person using the data visualisation screen can quickly identify the scenario. In this case, the COP is a successful command and control system in the military (Kookjin et al., 2023).

Recognising the cyber situation using easily understandable symbols is necessary to rapidly prepare for and respond to a cyber-attack. Kookjin et al. proposed using Cyberspace Symbol Components from the MIL-STD-2525D (Department of Defense, 2014). The CyCOP visualisation screen uses a common standard to express cyberspace objects as hexagons with symbols or characters. MIL-STD-2525D proposes a versatile expression method utilising a frame, icon, and fill for graphic representation. This method can be used on accurate maps and cyberspace (Ibid).MIL-STD-2525D, a military symbology document, does not currently include cyberspace symbols for diverse entities and activities in COs. This provides network architecture, cyber threats, digital communication channels, and unique cyberspace-related elements for effective military planning and visualisation tools.

Cyber commanders and planners must understand COs to visualise end states and describe intent, especially in Offensive Cyber Operations (OCO) (Bender, 2013). The U.S. Army is developing frameworks to visualise commanders' areas of operations in physical, cognitive, and virtual dimensions, enhancing their understanding of cyberspace opportunities, risks, and vulnerabilities (U.S. ARMY, 2013). Combining knowledge and visualisation techniques ensures commanders can navigate complex operational environments and respond to emerging threats.

Additionally, Klipstein's research demonstrated the effectiveness of an OCO risk framework with graphical outputs in aiding personnel needing more necessary experience, suggesting that these graphics mitigate the need for national-level experience (Klipstein, 2019).

Monitoring information systems and utilising visualisation techniques are essential for effective security strategies and operational planning (Goethals & Hunt, 2019). Advanced technologies can help visualise and predict battlespace, enhancing understanding of operational and environmental complexities (Bryant, 2016).

Colours enhance SA in cyberspace, aiding decision-making and understanding complex cybersecurity concepts through visual representation in cyberspace training (Dobson & Carley, 2021) (NIST, 2014). The NIST 2017 framework emphasises the importance of visualisation tools and communication skills in various cybersecurity roles, enabling efficient decision-making and collaboration in cyber operations planning (NIST, 2017). Decision makers are more confident and precise when given more choices, and modern cybersecurity operations must adapt to the technology industry's design and visualisation, focusing on contextualising data rather than attempting to visualise all available information (Ward, 2023). OCO planners can effectively utilise visualisation

to aid decision-making, enhance SA, and achieve operational goals by focusing on contextualising data rather than presenting all available information.

Graphic control measures in land domains can be adapted for SA in cyberspace, using offensive, defensive, and tactical mission graphics to depict actions (McCroskey & Mock, 2017). Wang proposes a method for creating a cyberspace map model using IP addresses, but further development and testing are required for practical application (Wang et. al., 2021). Wong et al. propose a framework for CSA, integrating it into a cyber operation planning tool for real-time monitoring, analysis, and decision-making (Wong et. al., 2021). Gutzwiller`s study highlights the need for enhanced training and skill development in Cyber Operations situational analysis and the effectiveness of user-centred design in addressing specific population needs (Gutzwiller et al., 2016).

Governments' proprietary cyber operations tools like Argos software demonstrate advanced monitoring and defence capabilities. They visualise cyberspace for governments, businesses, and individuals and indicate significant offensive cyberspace capabilities (Innovation Development Institute, 2009). Another tool, the Cyberspace Effects Server, provides comprehensive cyberspace visualisations for mission planning and execution tasks, enhancing understanding of COs and kinetic domain tactics. Still, it requires further integration for enhanced effectiveness (Hasan et al., 2021).

3.3 Frameworks Guiding Cyberspace Operations

The operational framework is a cognitive tool that aids commanders in visualising and describing combat power applications, enhancing decision-making, communication, scenario planning, training, and SA (Army Techniques Publication, 2024). NATO's Allied Joint Doctrine for Cyberspace Operations guides joint operations planning and assessment, integrating voluntary cyber effects from allies into Alliance missions (AJP-3.20, 2020) (Goździewicz, 2019). COs significantly impact military operations, but cyber operational planning has not been fully addressed in the past decade. Clear objectives and historical analyses are needed for new CO strategies (VanDriel, 2016). COs necessitate understanding system posture, adaptation to adversaries, and data-driven operations to address dynamic assets, complex communication paths, and new attack surfaces (Ziring, 2015). A 2013 US Army white paper presents the LandCyber framework, a unified operational and institutional solution for Army COs from 2018-2030, focusing on unified COs and enhanced understanding (U.S. ARMY, 2013). The US military is exploring the Trilateral Strategic Initiative (TSI) to develop an agile operational assessment framework for IT, acquisition, and COs, enhancing interoperability and trust (Bryant, 2016).

Cyber-FIT Version 4 is a simulation framework for cyber team performance modelling, addressing contested environments' cyber mission forces. Agile software development processes such as Scrum and DevSecOps optimise cyber range planning, managing new technologies, vulnerabilities, and patches, and supporting CO plans (Dobson & Carley, 2021) (Carroll, 2023).

Over the past two decades, scientific research on DCOs has primarily focused on developing techniques, algorithms, and constructs to support active and passive efforts (Goethals & Hunt, 2019).

The NIST Special Publication aids in security control assessments and risk management, focusing on IT/cybersecurity personnel in Federal Organizations. It also includes the Cyber Operational Planner speciality area, enhancing cybersecurity personnel's understanding and mitigating risks within their organisations. Integrating cybersecurity principles, risk management, and operational requirements into training and planning processes enhances readiness for complexities (NIST, 2014) (NIST, 2017).

Sulin's study examines how non-state actors such as Anonymous used cyber-attack methods in their 2016 campaign and compares them to established frameworks. The canonical model of OCOs provides a comprehensive overview, but future research needs accurate frameworks, post-attack analysis, and larger-scale analysis (Sulin, O, 2018).

Klipstein's paper uses decision-maker preferences, risk analysis, and simulation modelling to aid commanders in OCOs, especially for inexperienced personnel. It offers practical insights, but more holistic frameworks are needed (Klipstein, 2019).

The study by Kookjin et.al. (2023) suggests that enhancing CSA through the Cyber Common Operational Picture Framework can aid military and private sector cyber defence training. It emphasises the importance of recognising cyberspace, addressing planning gaps, enhancing SA, focusing on operational-level improvements, and integrating cyberspace into planning processes.

The U.S. Army Techniques Publication offers a comprehensive approach to CO Planning, including cyberspace layers, terrain analysis, threat description tables, terrain effects matrix, event matrix, hybrid threat analysis, and hybrid threat analysis, ensuring effective COs and security for operational-level decision-making (Army Techniques Publication, 2024).

3.4 Integrating Situational Awareness in Cybersecurity Visualisations

Standard rules for symbol construction and generation are needed for joint military symbology. Ineffective communication between cyber and physical domain warriors hinders the practical application of operational campaign design and war principles in COs. Cyberspace operational graphics can help cyber planners and operators communicate mission-relevant information to warfighters unfamiliar with the technical details of cyberspace, potentially leading to the identification of parallels and analogies in the physical domain (McCroskey & Mock, 2017).

This study examines visualisation techniques for CSA in military contexts, focusing on operational-level staff. It highlights a gap in understanding stakeholders and information types in visualisations. It emphasises the importance of SA for timely decision-making and the need for more scientific research on CSA visualisations. It suggests designing CSA visualisations based on user needs and preferences, reducing complexity and allowing easy sharing (Jiang et al., 2022).

This paper discusses the need for more research on situation awareness in Security Operation Centres (SOCs), highlighting the need for more theoretical foundations and understanding of its impact on human operators' performance. It suggests further investigation and exploration of tools for operationalising SA (Ofte & Katsikas, 2023). Advanced visual tools should incorporate predictive analytics for real-time threat forecasting and vulnerability identification, enhancing decision-making capabilities, such as network maps, in detecting and managing cyber threats (Barford et.al., 2010). Franke and Brynielsson emphasise incorporating human factors into cybersecurity, advocating for real-time visualisation tools to provide contextual information about threat severity and potential impacts (Franke & Brynielsson, 2014). Renaud and Ophoff suggest that CSA tools should be user-friendly and practical, guiding users through security information interpretation and response strategies (Renaud & Ophoff, 2021).

The final paper in this review highlights the importance of human-to-human communication in cyber defence decision-making and identifies inefficiencies in security operations. It suggests that 3D mixed reality visualisation can enhance CSA without directly impacting decision-making processes, highlighting the need for further research (Ask et al., 2023).

This section explains the requirement to develop advanced visual tools and standardised symbology for command-and-control systems to bolster joint military operations. Such enhancements are essential for improving SA and facilitating more effective decision-making in CO.

3.5 User Requirements From the Literature Review for the Cyber Planner Tool

This subsection outlines the essential user requirements and compatibility features necessary for the effective deployment and operation of the Cyber Planner tool, as detailed in the literature review chapter.

The Cyber Planner tool is crucial for COs, enhancing commanders' understanding of cyberspace activities. It should interface with established frameworks like AJP-3.20, LandCyber, and NIST recommendations (AJP-3.20, 2020) (U.S. ARMY, 2013) (NIST, 2014). Advanced visualisation tools facilitate interoperability and offer decision assistance (McCroskey & Mock, 2017)(Klipstein, 2019) (Bryant, 2016). The tool should incorporate risk management frameworks, support DCOs, analyse political conflicts, and offer decision assistance (Wong et. al., 2021) (NIST, 2022). It should provide real-time information management, a comprehensive operational picture, context-dependent awareness, integration with security awareness principles, icon design, and threat behaviour analysis (AJP-3.20, 2020) (Venables, 2021) (Dobson & Carley, 2021) (Kookjin et.al, 2023) (NIST, 2014). It should also offer comprehensive visualisation capabilities, contextualised information representation, military symbology, 3D mixed reality visualisations, automated frameworks, and tailored training for cyber operations analysts and planners (Mohite, S, 2018) (Wong et. al., 2021) (Gutzwiller et. al., 2016) (Hasan et. al, 2021). The tool should also incorporate predictive analytics, dynamic data presentation, and human factors to make complex data comprehensible to operators in real time (Ask et al., 2023). It should be designed with practical and user-friendly features that align with the resource constraints of small and medium enterprises (Renaud & Ophoff, 2021). This review emphasises the need for standardised frameworks, improved CSA, sophisticated visualisation tools, and user-specific modifications for successful CO planning and execution.

The literature review identified key user requirements for a CO planning tool, including real-time threat monitoring, cyber terrain mapping, interoperability with military command structures, and decision-support mechanisms. Comparison of Tools and Frameworks for Cyber Operations Planning shows a table comparing the identified tools and frameworks for relevance (Arik, 2025).

4. Results of Interviews

Semi-structured interviews were conducted with XS 2021 Higher Command, Cyber Headquarters (CHQ) staff officers, and Tactical Commanders to gather contextual and nuanced information about operational, technical, and strategic subjects. Interviews were conducted with six cyber operations professionals with varying IT, cybersecurity, and military operations backgrounds. This sample represents a focused subset of cyber operators, though its representativeness relative to the total population remains an open question. The recruitment process involved selecting experienced professionals engaged in CO exercises, ensuring relevant insights into operational planning challenges. Inquiries were made about the participants' professional backgrounds, the XS 2021 exercise's planning methodology and particular user needs for a Cyberspace Operations Planning Tool. Their answers emphasised the need for more excellent data visualisation, better interaction with standard frameworks, more situational awareness, and gaps in the existing operational tools. After analysing the responses, the researcher found recurrent themes and demands incorporated into the survey for broader validation.

The study explored the CHQ planning process in the XS 2021 exercise and user requirements for the CO Planning tool through a methodical process including research objectives, literature review, expert consultation, and semi-structured interviews. The interviews focused on the interviewee's background, planning process, and tool requirements. The interviewees had IT, cybersecurity, military operations planning, and security architecture degrees. They had at least eight years of CO experience and planned CO exercises, and they are currently involved in higher-level planning, cybersecurity architecture research, and security operations centre management. The following summarises the proposed user requirements for the Cyber Planner Tool.

The CO Planning Tool should include layers for a comprehensive view of the cyber environment, filters for quick connections, and colourful, easy-to-understand symbols. The tool should display asset properties and information when the user moves their mouse over it and allow them to combine physical assets into logical layers. The tool should be user-friendly, using symbols like standard ICT tools, and integrate seamlessly with existing frameworks. It should also feature automatic application programming interfaces for mapping tactics to frameworks such as MITRE, robust filtering options, and grouped networks for easy viewing. MITRE ATT&CK® is a globally accessible knowledge base for adversary tactics and techniques used in private, government, and cybersecurity sectors for developing threat models and methodologies (MITRE, 2025).

Developing standard operating procedures (SOP) for COs can be challenging due to the divide between military and cyber backgrounds. A dual system can improve operational planning and streamline the process. The Cyber Planners tool should be a comprehensive management system integrating asset information and SA with configuration management database-like functionalities for inventory management and semi-automated updates. It should also incorporate filtering options for better management of network devices, information and communications technology assets, adversary units, and own units, as well as a geographical map for enhanced visualisation and operational capabilities.

Due to infantry-based approaches and technical details, the CHQ faces challenges developing SOPs. Staff procedures are insufficient for fast-paced COs; detailed task descriptions are needed for operations and planning cells. The Cyber Planners tool should be a comprehensive management system integrating asset information, SA, inventory management, and data exchange. It should also incorporate filtering options to manage network devices, ICT assets, adversary units, and own units better.

One interviewee needed a CO Planning Tool to analyse cyber and physical operational landscapes, including IT and risk management. The tool should identify vulnerabilities, align with forces' capabilities, and incorporate Allied Joint Doctrine joint functions. It should provide strategic-level information, assess risks, and catalogue critical assets. Universal symbols should be used to ensure understanding across command levels. The tool should enable real-time battle damage and operational assessments.

Another interviewee highlighted the challenges in the Cyber Command planning process due to the lack of integration and digitalisation. The process needed to be more cohesive and relaxed, requiring less time-consuming searches. She suggested a digital CO planning tool to streamline processes and enhance

operational efficiency. The proposed tool would address synchronisation issues in section briefings, ensure a clear understanding of operations, and improve timeliness. The Cyber Planners tool aims to enhance automation, integration, and real-time capabilities, reducing human error and improving efficiency. It should also facilitate report creation and coordination across tactical, operational, and strategic command levels.

A further Interviewee suggested a user-friendly COs Planning Tool with comprehensive information on adversaries' strategies and visual aids. The tool should integrate with platforms like MIPS, support precise targeting and planning, and be compatible with NATO planning systems. It should have strong filtering capabilities, automated reporting, and a chronological timeline.

The XS exercise highlighted the importance of a planning tool in the operations department. Operational processes can be improved, and standardised templates and better structuration are needed to enhance metadata management and data handling.

5. Proposed Enhancements for Operational Planning and Situational Awareness for COs

In XS 2020, the CHQ developed an operational plan for sub-units, focusing on the Military Decision-Making Process and improving procedures. However, the higher command realised the need to align the plan with the exercise timeline. The CHQ used open-source drawing tools for visual operational planning, allowing for SA and practical strategies to address cyber threats. In 2022, the CHQ adopted a new cyber exercise command structure and prepared the initial standard operating procedures.

By 2022, CHQ had evolved its cyber exercise command structure and introduced a preliminary version of standard operating procedures (SOPs). Additionally, it developed a Cyber Planner tool (Figures 2 and 3), introducing several enhancements:

- Advanced Filtering Options: The tool allowed planners to apply filters based on affiliation, targeting evaluation, targeting results, persona, and network devices.
- Enhanced Visualisation: New asset symbols with amplifiers improved clarity, while logical and dynamic asset connections provided a better operational overview.
- Targeting Assistance: The tool streamlined the targeting process, grouping Red Team units (considered Blue Team targets) in an organised layout (Figures 2 and 3).

Figure 2 provides a high-level view of the Cyber Planner tool, illustrating the operational environment used for cyberspace operations planning. The visual representation includes own forces, enemy assets, third-party elements, and cyber personas, each marked with distinct symbols and logical connections. The diagram highlights how planners interact with the tool to develop situational awareness and course-of-action (COA) strategies. Key features, such as dynamic linking of assets and real-time updates, support decision-making across strategic, operational, and tactical levels.

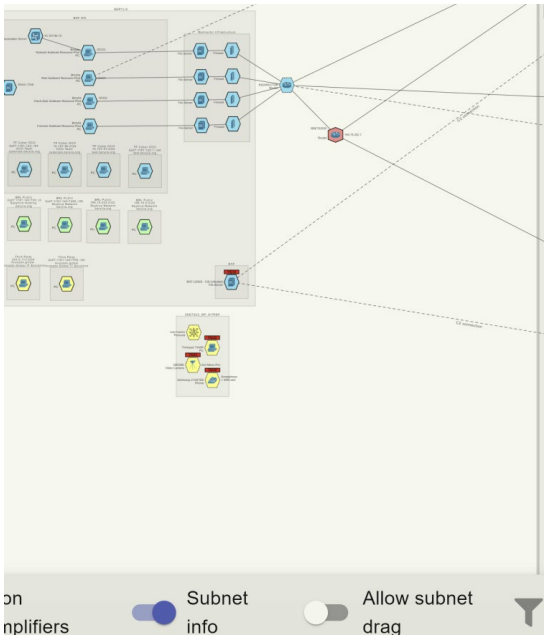

Figure 2: Proposed Cyber Planner tool with Blue team units

Figure 3 displays the Cyber Planner's user interface, explicitly showing Red Team units grouped as Blue Team targets. The left-side function menu includes various filtering options: affiliation, targeting evaluation, and network devices. The right-side control panel provides options to lock the screen, save the layout, and access settings. By zooming into key details, Figure 3 clearly depicts how planners interact with the system. These figures are an original contribution from the lead author, who created and modified the tool to optimise planning and execution procedures according to each team's unique requirements.

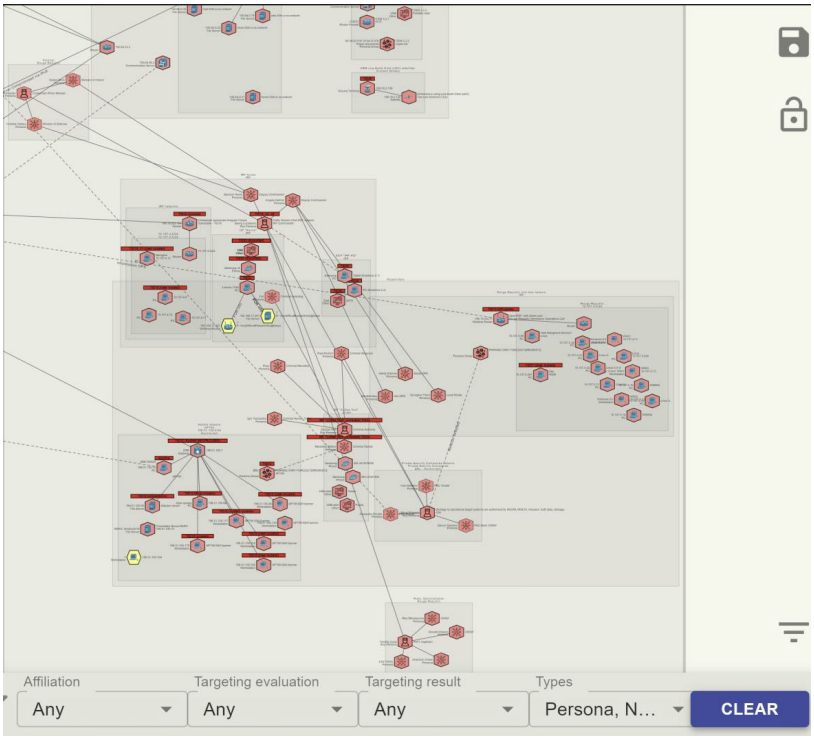

Figure: 3 Proposed Cyber Planner tool with Red team units

The tool assisted in identifying additional user requirements for future integration and acted as the first foundational test in CO planning. Even though it wasn't finished, it successfully illustrated how crucial logical connections, visual planning, filtering, and other aspects are to assisting with CO planning.

6. Results of Surveys

The survey validated 30 user requirements via Likert-scale responses from 22 cyber operations experts. A 70% agreement threshold confirmed most criteria for improving situational awareness and operational planning. Future validation is needed for real-time information management, human factors, API integration, and backend synchronisation. The dataset contains survey responses on cyber operations visual planning tools, with categorical responses. The histogram is presented in Figure 4.

The survey was completed by 22 participants from the NATO Cooperative Cyber Defence Centre of Excellence Integrating Cyberspace Considerations into Operational Planning Course. The survey's design, targeting specialised professionals from many nations, contributes to the findings' validity within the expert community. The identified and validated user requirements, their sources, and newly discovered ones are summarised in "User Requirements Validation for Enhancing Operational Planning and Situational Awareness in Cyberspace Operations" (Arik, Google Drive, 2025).

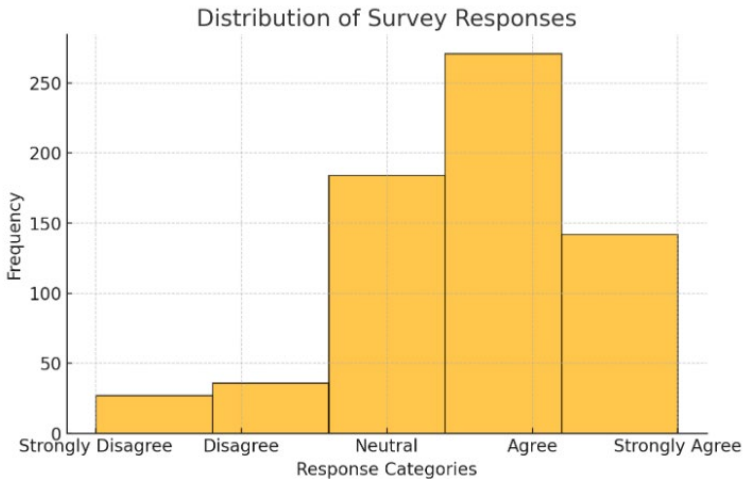

Figure 4: Distribution of Survey Responses on Cyber Operations Visual Planning Tool Features

7. Limitations and Future Work

The study's limitations include the interviewees being cybersecurity and military SMEs with at least eight years of experience in CO exercises and planning. The survey revealed four unvalidated user requirements, potentially compromising usability and efficiency. The 22-person sample size may be small for broad statistical generalisation but is strong in domains like COs. Future work will involve developing a CO visual planning tool and detailed planning processes.

8. Conclusions

The study effectively addressed the research questions by integrating findings from a literature review, expert interviews, and survey responses. It identified the logical, cyber-persona, and physical layers as essential to cyberspace operations. It demonstrated how their integration into a Cyber Planning Tool enhances operational planning and execution at multiple levels. Survey results confirmed that real-time operational visualisation tools improve CSA by providing explicit depictions of cyber assets and evolving threats, aiding decision-making. Additionally, 30 user requirements—validated by subject matter experts with over 70% agreement—highlighted the need for enhanced interoperability, automated asset tracking, and dynamic visualisation capabilities. These findings substantiate the necessity of advanced cyber planning tools for NATO and allied forces, confirming the study's conclusions with empirical evidence.

References

AJP-3.20. (2020, January). *ALLIED JOINT DOCTRINE FOR CYBERSPACE OPERATIONS.* https://www.gov.uk/government/publications/allied-joint-doctrine-for-cyberspace-operations-ajp-320

Army Techniques Publication. (2024, January 23). ATP 2-01.3, Intelligence Preparation of the Battlefield,Change No. 2,No. 2-01.3. Washington, DC, U.S.

Ask et al. (2023). A 3D mixed reality visualization of network topology and activity results in better dyadic cyber team communication and cyber situational awareness. *Sec. Cybersecurity and Privacy*, Online Volume 6 - 2023 | https://doi.org/10.3389/fdata.2023.1042783.

Barford et.al. (2010). Cyber SA: Situational Awareness for Cyber Defense. *In Cyber Situational Awareness*, 3-14.

Bender, J. M. (2013). The Cyberspace Operations Planner. *Small Wars Journal*.

Bryant. (2016). Mission Assurance through Integrated Cyber Defense. *Air and Space Power Journal*, 5-18.

Carroll, J. (2023). Agile Methods For Improved Cyber Operations Planning. *Proceedings of the 22nd European Conference on Cyber Warfare and Security, ECCWS 2023* (pp. 108-115).

Department of Defense. (2014, June 10). *JOINT MILITARY SYMBOLOGY.* http://everyspec.com/MIL-STD/MIL-STD-2000-2999/MIL-STD-2525D_50933/

Dobson, & Carley. (2021). *Cyber-FIT Agent-Based Simulation Framework Version 4.* Pittsburgh,: Center for the Computational Analysis of Social and Organizational Systems.

Endsley. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *The Journal of the Human Factors and Ergonomics Society, 37(1),*, 32–64.

Franke, & Brynielsson. (2014). Cyber situational awareness—A systematic review of the literature. *Computers & Security, 46*, 18-31.

Goethals & Hunt. (2019). A review of scientific research in defensive cyberspace operation tools and technologies. *Journal of Cyber Security Technology*, 1-48.

Goździewicz, W. (2019, November 11). *Cyber Defence Magazine*. Retrieved from Voluntarily by Allies (SCEPVA): https://www.cyberdefensemagazine.com/sovereign-cyber/

Gutzwiller et. al. (2016). A Task Analysis toward Characterizing Cyber-Cognitive Situation Awareness (CCSA) in Cyber Defense Analysts. *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, 14-20.

Hasan et. al. (2021). A Cyberspace Effects Server for LVC&G Training Systems. *2021 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC)* (pp. 1-12).

Innovation Development Institute. (2009). *Argos - Visualization Tool for Cyberspace Command and Control*. https://www.inknowvation.com/sbir/awards/af-2009-argos-visualization-tool-cyberspace-command-and-control

Jiang et al. (2022). Systematic Literature Review on Cyber Situational Awareness Visualizations. *IEEE Access, vol. 10*, 57525-57554.

Klipstein, M. (2019). Seeing is Believing: Quantifying. *THE CYBER DEFENSE REVIEW*, 88.

Kookjin et.al. (2023). Study on Cyber Common Operational Picture Framework for Cyber Situational Awareness. *Applied Sciences*, https://doi.org/10.3390/app13042331.

Kosmol, L. &. (2019). *ICT Usage in Industrial Symbiosis: Problem Identification and Study Design.* https://annals-csis.org/proceedings/2019/drp/pdf/323.pdf

Llopis et al. (2018). A comparative analysis of visualisation techniques to achieve cyber situational awareness in the military. *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, 1-7.

M.Arik. (2025, Jan 15). *Google Drive.* Mapping of Literature Sources to Research Questions: https://shorturl.at/nUd9g

McCroskey, & Mock. (2017). Operational Graphics for Cyberspace. *Joint Force Quarterly 85*, 43.

MITRE. (2025, Jan 15). *ATT&CK*. Retrieved from MITRE: https://attack.mitre.org/

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

Mohite, S. (2018, January 26). *Cybersecurity operations and the role of visualization, design, and usability.* Retrieved September 20, 2023, from https://medium.com/uplevel/how-design-visualization-and-usability-impact-cybersecurity-operations-61d854b5e2d3

NIST . (2022, May). *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

NIST. (2014). *A Role-Based Model for Federal Information Technology/Cybersecurity Training.* Virginia: U.S. Department of Commerce.

NIST. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* Gaithersburg,: U.S. Department of Commerce.

Ofte, & Katsikas. (2023). Understanding cyber situational awareness in SOCs. *Journal of Information Security and Applications, 62*, 102952.

Pfannenstiel, M., & Cox, D. (2024). NATO's Cyber Era (1999–2024) Implications for Multidomain . *MILITARY REVIEW ONLINE EXCLUSIVE · OCTOBER 2024*, 1-10.

Pullen, J. M. (2015). Visual planning for cyber operations. In M. O'Leary, *Cyber Operations: Building, Defending, and Attacking Modern Computer Networks* (pp. 221-239). Towson: Apress.

Renaud, & Ophoff. (2021). An SME-specific cyber situational awareness model to predict the implementation of cybersecurity practices. *Journal of Cybersecurity*, 24-46.

Sulin, O. (2018, FEB 16). CYBER ATTACK CAMPAIGNS IN POLITICAL CONFLICTS. Turku, Finland. https://www.utupub.fi/handle/10024/145536

U.S. ARMY. (2013). *THE U.S. ARMY LANDCYBER WHITE PAPER 2018-2030.* Fort George G. Meade,: U.S. Army Capabilites Integration Center.

VanDriel, M. (2016). Bridging the Planning Gap: Incorporating Cyberspace Into Operational Planning. *The Cyber Loop*, Online [http://thecyberloop.com/journal-article/].

Venables, A. (2021, November 16). *Frontiers in Education*. Retrieved from Modelling Cyberspace to Determine Cybersecurity Training Requirements: https://www.frontiersin.org/articles/10.3389/feduc.2021.768037/full

Wang et. al. (2021). *CYBERSPACE MAP MODEL CREATION METHOD AND DEVICE.* Houston: Patent Application Publication.

Ward, P. (2023). Choice, Uncertainty, and Decision Superiority: Is Less AI-Enabled Decision Support More? *IEEE TRANSACTIONS ON HUMAN-MACHINE SYSTEMS, VOL. 53, NO. 4, AUGUST 2023*, 781-791.

Wong et. al. (2021). A Framework for Measuring Situation Awareness in Cyberspace Operations. *Proceedings of the Human Factors and Ergonomics Society Annual MeetingVolume 65, Issue 1*, 358-362.

Ziring, N. (2015). The Future of Cyber Operations and Defense. *Journal of Information Warfare*, 1-5.