Using Wargaming to Model Cyber Defense Decision-Making: Observation-Based Research in Locked Shields

Pietari Sarjakivi, Jouni Ihanus and Panu Moilanen
University of Jyväskylä, Finland

pietari@sarjakivi.fi
jouni.e.i.ihanus@student.jyu.fi
panu.moilanen@jyu.fi

Abstract: Defensive Cyber Operations (DCO) in complex environments, such as cyber wargames, require in-depth cybersecurity knowledge and the ability to make quick decisions. In a typical DCO, execution rarely follows a pre-planned path because of extensive adversary influence, challenging an already complex decision-making environment. Decision-making models have been extensively studied from perspectives of military operations and business management, but they are not sufficiently researched in the context of cyber. This paper responds to this need by examining the decision-making models of DCO leaders in a live-fire wargame environment. This study was conducted by observing leaders of cyber operations during the world's largest live-fire cyber exercise, NATO Locked Shield 2023. In this exercise, the blue teams plan and execute their defensive cyber operation in a realistic operational environment, while the red team conducts attacks against the defended environment. The large-scale, wargaming-style environment of Locked Shield is one of the best environments for modelling DCO decision-making models; in this exercise, the DCO is broad and multi-faceted, a perspective which cannot be achieved in a typical capture-the-flag competition or a single security incident. DCO leaders must be able to manage two distinct decision-making processes with different sets of required skills to be successful in the mission. While the primary process relates to the execution and evolution of the pre-designed plan with traditional operational leadership skills, the secondary process deals with unplanned and deliberately caused cyber-related events that require a deep understanding of cybersecurity. In this respect, the main contribution of this research is the constructed decision-making model of the DCO leader. This model is based on observations collected and presented in the context of multiple well-known decision-making frameworks. This model can be further used to train future DCO leaders and assess artificial intelligence's usability to support and automate decision-making in such operations.

Keywords: Decision-Making, Defensive Cyber Operations, Wargaming, Locked Shields

1. Introduction

Ubiquitous digitalisation and connected societies have emphasised the importance of the cyber dimension. In a military domain, one indicator of this development is NATO's decision to recognise cyberspace as a domain of operations alongside the traditional domains of air, land, and sea (NATO, 2021b). The digital footprint of different organisations is increasing, as are adversaries' actions. This development can be seen in both the volume and the sophistication of the attacks, which increases the complexity of defensive measures (Fortinet, 2022; Microsoft, 2023). Identifying security breaches in cyberspace typically takes weeks (Mandiant, 2023) or months (IBM, 2023) - longer than in other domains. This is due to the complexity of the cyber domain compared to other domains.

The Defensive Cyber Operation (DCO) organisation can structurally be divided into multiple levels depending on several variables. Typical civil side Security Operations Centre (SOC) is divided into management levels and analyst tiers with different responsibility areas. This approach can be widely scaled based on the size of the areas of responsibility dedicated to the SOC and other organisational variables (Knerler et al., 2022). On the military side, the structure of the cyber operation organisation similarly depends on a defined mission. However, similar management and analyst-level roles can be recognised in both organisation models (Dalmjin et al., 2020). In previous studies, this has been approached relatively widely: At the analyst level, D'amico et al. (D'Amico et al., 2005) and Gutzwiller et al. (2016) (Gutzwiller et al., 2016) have analysed the tasks and operating environment that experts encounter in their cyber security roles. Their studies are based on a cognitive task analysis that strongly focuses on cognitive challenges to create cyber situation awareness at the analyst level. Complex dynamic operating environments can strain human cognitive capabilities, challenging security analysts' ability to understand situations and make related decisions (Druzdzel & Flynn, 2010; Endsley, 1995). Machine learning can support human analysts in creating situation awareness and decision-making. The elements of the unknown are more common in defensive than offensive cyber operations, as DCOs rarely follow pre-planned paths due to the extensive adversary influence (Williams, 2014).

Wargaming exercises simulate real-life environments where players' decisions impact gameplay. They provide participants with the opportunity to gain experience and the possibility to experiment with different strategies

against other players. For researchers, they offer an excellent platform to observe decision-making in a realistic environment (Nesbit et al., 2013).

This study aims to understand the decision-making process during the DCO based on the Locked Shields cyber wargame type exercise. The research was conducted in a military context, but its results can also be utilised in civilian operations. The main contribution of this research is the constructed decision-making model of the DCO leader.

The paper is organised as follows: Section 2 introduces the research methodology, Section 3 presents the ontology of related decision-making models, Section 4 presents the observed environment, Section 5 introduces the construction of the model, and Section 6 concludes the study with future research topics.

2. Methodology

In terms of methodology, the study can be divided into two main stages, shown in Figure 1. These stages can be considered at the top level to include data collection and data analysis.

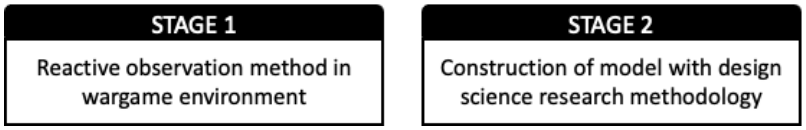

Figure 1: Research methodology utilised in this study

In the first stage, the authors observed the Blue Team (BT) Finland in the world's largest live-fire cyber exercise, NATO Locked Shield 2023, using the reactive observation method (Arthur, 2012, pp. 165–169). Observations were made during the live-fire exercise and in the preparatory phases. In addition, the data collected was supplemented by an interview survey conducted at different levels of the target organisation. This method was appropriate because all internal team communications were conducted via a game-like voice communication system, allowing the observers to listen to any conversation during the exercise freely. Regarding content knowledge, BT Finland performed well in this exercise, which is why the team's decision-making ability can be considered good and, therefore, suitable as the target of this study.

In the second stage, the authors used design science research methodology with a constructive research approach (Peffers et al., 2007) to create a constructive model for decision-making in DCO. The constructed model builds on known decision-making frameworks while providing an innovative structure applicable to operations with an active adversary. The methodology was chosen based on the nature of the subject of the study as a real-world problem that the proposed construct was intended to solve.

3. Decision-Making Frameworks

To develop decision-making in DCOs, it is essential to understand the structure of decision-making in their context. This chapter presents key elements in DCOs and relevant decision-making frameworks used in model construction.

3.1 Understanding Elements of Defensive Cyber Operations

For at least 200 years, military theory has divided decision-making in war into strategic, operational, and tactical levels, where the main difference between levels is the reach and timespan of the effect (Maxwell, 1997). Many Western militaries utilise a mission command model originating from the same era. The mission command is a decentralised model where the commander communicates the intent to subordinates, who then make decisions and act accordingly. The model is based on mutual trust, where the commander trusts the subordinates' skills and willingness to make decisions best fitting to the communicated intention, and subordinates trust that the commander has given the right direction and enough resources to complete the task. The idea behind the model is that the person closest to the action should have the most up-to-date understanding of the situation and, therefore, be able to make the right decisions (Storr, 2003).

DCO leaders and operators utilise the Cyber Situational Awareness (CSA) process to understand the operating environment's state to support decision-making in cyber operations. Inputs can be collected from technical sources like log management systems, endpoint and network sensors, honeypots and availability monitors (Husák et al., 2022) and non-technical sources like human observations (Vielberth et al., 2019). Situational

awareness is built with the perception of the current situation, comprehension of the current situation and projection of future status (Endsley, 1995). The Holistic Operational Framework for Establishing Situational Awareness in Cyberspace (HOFESAC) model categorises CSA information into six classes that together form a comprehensive understanding of operating environment: Threat environment, anomalous activities, vulnerabilities, key terrain, operational readiness, and ongoing operations (Dressler et al., 2012).

As Sun Tzu stated almost 2500 years ago, in combat situations, decision-makers must understand both their adversary and themselves (Giles, 1910). Cyber Threat Intelligence (CTI) is a process that provides information about adversaries, their tools, techniques, and procedures (TTP), as well as potential security threats. It utilises scenario thinking to produce strategic insights and potential courses of action (COA) that decision-makers can utilise in their planning and decisions (Schlette et al., 2021). Analysis of Competing Hypotheses (ACH) is one of the tools used to compare scenarios to identify the most likely COA (Lemay & Leblanc, 2018).

3.2 Relevant Decision-Making Frameworks

To model the decision-making process in DCO, two well-known frameworks were used: Cynefin and OODA. Both frameworks are widely used within cybersecurity. Cynefin operates at a high level of abstraction and is a well-suited framework for modelling decision-making, as all four contexts with their respective natures are present in major cyber incidents (B. S. Dykstra & Orr, 2016). As a whole, cybersecurity can be recognised as a complex system (Valentine, 2018). The OODA loop framework, originally designed for combat situations, is well-suited for rapid decision-making by cyber operators (Husák et al., 2022). These frameworks are introduced below.

The cynefin framework is a sensemaking tool applied to a broad range of industries. It recognises four different contexts for decision-making:

1. In a simple context, decision-making is based on best practices, and the situations are relatively straightforward, as clear causality is easy to find.
2. In a complicated context, causality is present, but an expert is needed to analyse the situation and select the most suitable out of multiple right choices.
3. In a complex context, there is one right choice, but the context is almost impossible to map entirely, and the decision-maker must manoeuvre with a limited understanding of the situation.
4. In a chaotic context, no clear causality can be found in a reasonable time, and there are too many moving elements to make fact-based decisions. In a chaotic context, decision-makers must both act with the best available information and work to shift the context to complex (Snowden & Boone, 2007).

The OODA loop is a combat operations process developed to support fast decision-making and "expose flaws of competing or adversary systems" (Boyd, 1986). Its developer, Air Force Colonel John Boyd, was a fighter pilot who studied previous conflicts, and this decision-making model has been widely adopted within Western militaries (Osinga, 2005). OODA loop includes four phases that are repeated in a fast closed loop.

1. In the observation phase, data is collected from the environment.
2. In the orientation phase, data is analysed, and comprehension is created.
3. In the decision phase, the alternative COAs are reviewed, and the preferred COA is selected.
4. In the act phase, the decision is implemented into an action. (Husák et al., 2022; Osinga, 2005).

4. Observations from Locked Shield

4.1 Describing the Observation Environment

Locked Shields is the world's largest international cyber defence exercise. This annual exercise "enables cyber security experts to enhance their skills in defending national IT systems and critical infrastructure under real-time attacks". It has been organised by the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) since 2010. In 2023, over 2000 cyber experts from 32 nations participated in the exercise (NATO Cooperative Cyber Defence Centre of Excellence, 2023).

Locked Shields is a traditional Red Team (RT) versus Blue Team(BT) exercise where the RT acts according to the pre-planned scenario and has the right to perform OCO while the BTs' Rules of Engagement (ROE) limit them to DCO (NATO Cooperative Cyber Defence Centre of Excellence, 2023; Williams, 2014). This ROE is realistic from a legislative point of view but creates an imbalance between actors and always keeps the initiative with the red

team. This imbalance creates a need for strategic analysis and CTI in case the BTs want to participate actively in the exercise.

By their nature wargaming exercises provide participating BTs a clear objective for their mission and a scoring mechanism that can be used to measure how successful teams have been. Time compression forces teams to react quickly and under pressure. The scoring system adds an element of competition to the exercise, enabling participants and researchers to evaluate the effectiveness of decisions made. After Action Reports (AAR) shared with participants after the execution, make it possible to compare different approaches teams take. By studying real-life cyber incidents that lack the scoring system and the possibility to compare approaches different teams take or Capture the Flag competitions that lack realistic large-scale environments, the modelling of decision-making is challenging. For those reasons, the large-scale, wargaming-style environment of Locked Shield is one of the best environments for observing DCO decision-making.

4.2 Observations of Decision-making

Figure 2 shows the key observations made during the exercise.

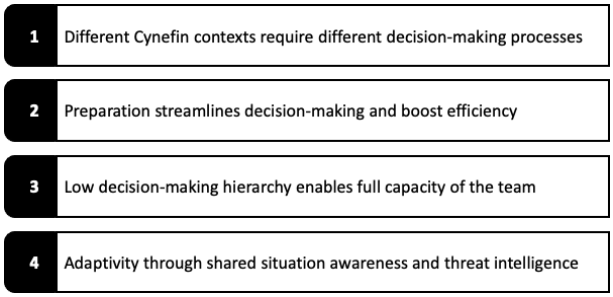

Figure 2: Key observations from the exercise

The first observation is that decision-makers in DCOs must operate constantly in multiple Cynefin contexts, each requiring a different set of skills. The speed and process of decision-making also vary between different contexts.

The second observation highlights the importance of preparations in building readiness for operations and efficient decision-making. Finland was one of the smallest high-performing blue teams (NATO Cooperative Cyber Defence Centre of Excellence, 2022). The BT Finland was primarily based on reservists who spent longer than average preparing for the exercise (NATO Cooperative Cyber Defence Centre of Excellence, 2022). The preparations include developing and familiarising with joint tooling and processes, studying the mission and scenario, and practising critical phases of the execution.

The third observation relates to the effectiveness of low hierarchy decision-making with the mission command model utilised by BT Finland. Figure 3 presents the command structure, roles, and responsibilities in BT Finland. BT Finland had two operations leaders who worked in shifts, one leading the operation execution whilst the other preparing plans for the next phase that he was going to execute. The operations plan was built with an ideology where every squad had complete responsibility for their sector in the defended environment, and as long as a joint tool, techniques and procedures were followed, squad leaders had the freedom to execute tasks in their sector as they felt appropriate. Squads' tasks were divided among cyber operators whose responsibility was typically limited to certain functions like administration, threat hunting or countermeasures; or special systems like electric power grid or air defence system.

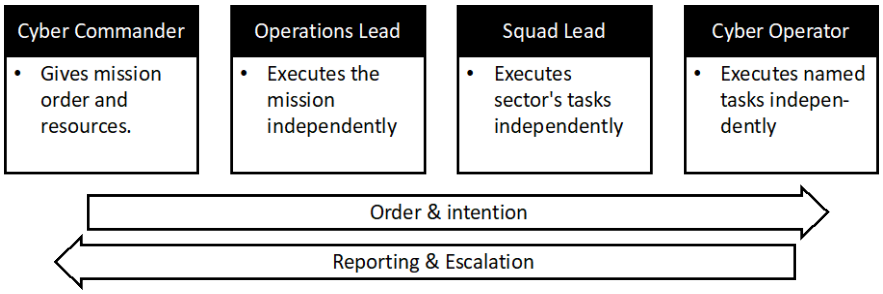

Figure 3: Command structure, roles, and responsibilities in Blue Team Finland

The fourth observation pertains to the significance of sharing CSA and CTI with the entire team in real time and with a high level of detail. In addition to advanced technical tooling for sharing detailed CSA, the BT had hourly situation briefs for leaders and a dedicated Tactical Operations Centre (TOC) led by operations leaders acting as a fusion centre. TOC had a CTI function producing analysis of possible Courses of Action (COA), which TOC used to provide early warning for the need to balance the resources to prepare for upcoming attacks dynamically. In a large-scale exercise like Locked Shields, the BTs must make decisions with a limited understanding of the complex operating environment and be prepared for upcoming unknown unknowns.

5. Construction of Model

According to the observations presented in the previous chapter, decision-making in the DCO can be divided into two distinct processes, as shown in Figure 4. The primary process relates to the execution and evolution of the pre-designed plan using traditional operational leadership skills. The secondary process deals with unplanned and deliberately caused cyber-related events, requiring a deep understanding of cybersecurity.

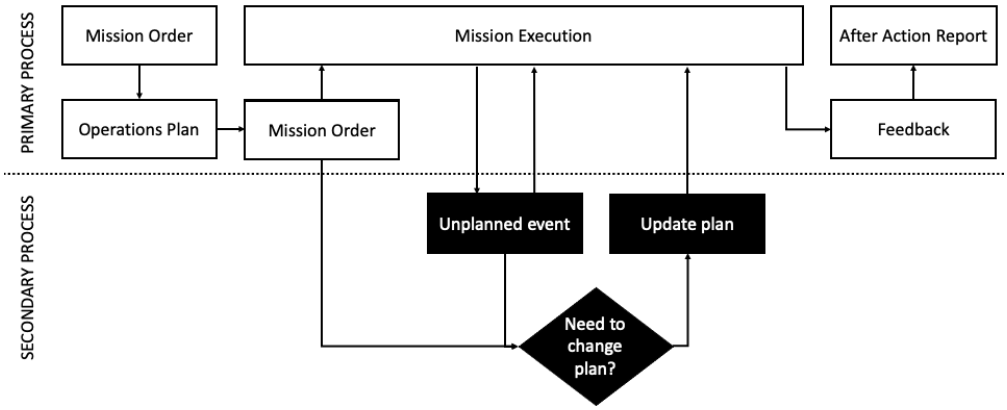

Figure 4: Two distinct decision-making processes in the defensive cyber operation

5.1 The Primary Process

The primary process aims to accomplish the mission according to the plan. It operates mainly within the simple or complicated context of Cynefin framework and follows traditional management structures and best practices such as Project Management Body of Knowledge (PMBOK) (Project Management Institute, 2021) and the NATO Comprehensive Operations Planning Directive (COPD) (NATO, 2021a). For a DCO leader to be successful in the primary process, at least the following good management attributes are needed: Clear vision, strong team-building skills, good communication skills, can-do attitude, and discipline (Pennypacker & Cabains-Brewin, 2003). Planning effective cyber operations needs to take nested technical aspects of planning into account, and therefore, an understanding of the cybersecurity domain is needed (Barber et al., 2015). The DCO leader may seek support from team members or external experts, so these attributes are not essential for the DCO leader.

The mission order defines the mission's objectives, ROE, and resource limits. The mission order is influenced by prior strategic decisions such as the importance of cybersecurity in the political agenda, the technological education the nation provides to its citizens, local legislation's maturity to recognise cybercrime and surveillance, partnership with the private sector, and overall digitalisation maturity of the country. The political and financial state of the organisation and prior events, such as previous cyber operations and synchronised military operations, influence the mission order.

After receiving the mission order, the DCO leader and the closest leaders craft an operations plan defining prioritised mission sub-objectives, execution plan, timeline, available support, organisation, and responsibilities. Operational planning must analyse environmental components to understand connections and dependencies and identify high-priority components (Barber et al., 2015). The plan is developed further in the organisation, according to the mission command model, and rehearsed to ensure execution readiness. DCO organisations must utilise joint tools, techniques, and procedures that are interoperable with possible allied forces and set the roles in a way that every member of the team is in the optimal role for them. Development ideas and lessons learned from previous operations should be considered to improve organisations' capabilities further. Decision-making in the planning and rehearsing phases is not as time-critical as in later phases but might lack information about the upcoming mission and operating environment. Therefore, DCO leaders should use this time wisely

and utilise CTI to get as much information about the environment and adversaries' centres of gravity as possible to make the right decisions for the plan.

The mission execution follows the operations plan as well as possible, although it is likely that time constraints in planning and complicated cyber context create a need for adaptability. Primary process decisions in the execution phase need a good understanding of operations progression, and for example, DCO leaders need to decide when a task is ready enough for the team to continue forward, what activities can be left undone for now to catch the timeline, how to re-allocate resources to optimise team's performance, and which tasks to prioritise. Threats are detected through CSA and mitigated with practised processes. Accurate CTI gives time for defenders to prepare for attacks.

After execution, the team gives and receives feedback from each other and other stakeholders. If DCO was conducted in a wargaming environment, scoring could be used to measure the outcome partially. Feedback is refined to development initiatives, which are, together with feedback, collected for AAR. The AAR is shared with a broader audience to share the lessons learned.

5.2 The Secondary Process

The secondary process is initiated when an unplanned event occurs, and its goal is to minimise this event's impact on operations plan execution within the primary process. In DCOs, unplanned events are often deliberately caused by active adversary actions. While traditional military operations studies recognise similar unanticipated events caused the need to change the plan, like German Field Marshal Moltke stated in the late 1800s (Kenny, 2016), the cyber domain offers exceptional elements of speed and uncertainty, and therefor this secondary process deviates from traditional military operations. Similarly, due to the cyber domain's highly interlinked nature and complicated environments where adversaries are difficult to recognise, this secondary process operates within the complex context of Cynefin.

The resolution of the situation can be mitigation of the unplanned event's impact through countermeasures and/or change of operations plan by, for example, re-prioritising the mission objectives, changing the resourcing balance of squads to focus the force or initiating a new special operation. To be successful in this secondary process, DCO leaders need a deep understanding of cybersecurity, a clear understanding of overall mission objectives, good intuition, and readiness to adapt to new situations quickly.

Dynamic decision-making in fast-changing situations must be based on prioritised mission sub-objectives, accurate CSA, and real-time CTI, as presented in Figure 5. CSA provides an understanding of the state of its own operations and operating environment, including incidents and unplanned events causing the need to start the secondary process. CTI provides strategic analysis of the adversary's mission and predicted COAs. As the need to make decisions evolves rapidly, the CSA and CTI information must constantly be available and up-to-date. Decision-makers must weigh different options based on available information and predicted outcomes to make the best possible decision. While defenders are often in reactive mode as adversaries have the initiative through the offensive nature of their operation, with CTI defenders can, for example, build deceptions, extra layers to defence, change the environment to break adversary's cyber kill chain and re-arrange their forces to lower the impact of the adversary's offence (Barber et al., 2015).

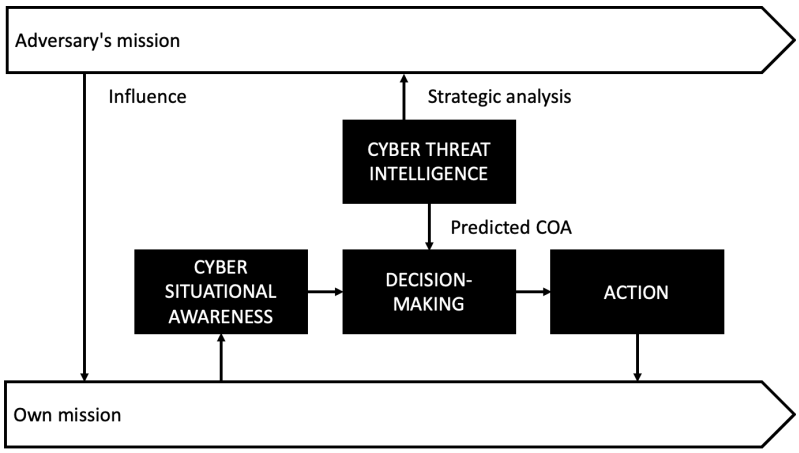

Figure 5: Dynamic decision-making in the secondary process

In complex contexts, the speed of decision-making is often crucial. While active decisions are needed promptly, a decision to wait for more information or a better time to react is a valid option, especially with an active adversary. As after intrusions, adversaries operate in a defended environment expecting to get caught, may defender's hasty decision to partially mitigate the threat just causes the adversary to lay low in the environment, making the complete mitigation difficult. The decision to mitigate the threat that has had time to build persistence and is unaware of the detection must be taken only when the defender is ready to completely take down the threat vector.

Although DCO leaders are the primary consumers for CSA and CTI, it is crucially important to share the information upward in the command chain, laterally to allied forces, and downwards to squads and cyber operators. Upstream sharing often happens through reports, but lateral and downstream sharing needs to have a fast and detail-oriented technical solution that can be integrated into technical defence solutions, being then easy to consume in rapid situations.

Cyber Operators' actions closely follow Boyd's OODA loop's principles as they, like fighter jet pilots, focus completely on the task they are performing at the time. Most of the tasks these cyber operators are given should be manageable independently or in small groups to maintain this high focus and speed up the closed OODA loop. Compared to fighter jet pilots, who can identify their enemy relatively easily, cyber operators must spend an enormous amount of time on anomaly detection and finding traces and potential future footholds of their actively hiding adversaries. Cyber operators must actively share information they feel is relevant, and therefore, they contribute to CSA more than they consume in the Orientation phase. For example, a filename seen in forensics investigations may lead to the detection of an adversary's foothold in a completely different system. In DCOs, cyber operators' anomaly detection skills, building relations between things they see, and intuition are essential assets that are improved through gained experience and effective information sharing.

6. Conclusion

Defensive Cyber Operations play a crucial role in safeguarding today's critical infrastructure. Decision-making in these operations is an essential element of success. To understand and develop the decision-making chain, one needs the opportunity to observe an appropriate operational environment. In this study, the NATO Locked Shields exercise was used as a platform to seek this information. This environment provides a wargame environment in the military context that emphasises the time compression and national crisis management elements. Observations were made based on several commonly known decision-making frameworks. In conclusion, this study proposed a dual-process model for decision-making in DCO. The authors argued that successful DCO leaders must be able to perform both primary processes simultaneously. This model can be further used to understand the DCO decision-making structure and train future DCO leaders.

For further research, it is important to evaluate the usability of the presented construction model in real DCO. The construction model can also be used to further assess the possibilities of AI-based decision-making at different stages of the decision-making process in such operations. It should be noted that regardless of the methodology used, there is always a risk of subjectivity in the observation method. For this reason, the possible need to supplement the findings should be borne in mind.

Acknowledgements

The authors would like to thank the Finnish Defence Forces and the National Defence Training Association of Finland for the opportunity to observe the Finnish Blue Team in the Locked Shields exercise and Business Finland for supporting the writing of this article (grant number 671/31/2022).

References

Arthur, J. (Ed.). (2012). *Research methods and methodologies in education*. SAGE.

B. S. Dykstra, J. A., & Orr, S. R. (2016). Acting in the unknown: The cynefin framework for managing cybersecurity risk in dynamic decision making. *2016 International Conference on Cyber Conflict (CyCon U.S.)*, 1–6. https://doi.org/10.1109/CYCONUS.2016.7836616

Barber, D., Bobo, T., & Strum, K. (2015). Cyberspace Operations Planning: Operating a Technical Military Force beyond the Kinetic Domains. *Military Cyber Affairs*, *1*(1). https://doi.org/10.5038/2378-0789.1.1.1003

Boyd, J. (1986). *Patterns of Conflict*.

Dalmjin, A., Banse, V., Lumiste, L., Teixeira, J., & Balci, A. (2020). *Cyber Commanders' Handbook* (pp. 24–30). NATO CCDCOE Publications.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *49*, 229–233. https://doi.org/10.1177/154193120504900304

Dressler, J., Moody, W. C., & Koepke, J. (2012). *A Holistic Operational Framework for Establishing Situational Awareness in Cyberspace*.

Druzdzel, M., & Flynn, R. (2010). *Decision Support Systems*. https://doi.org/10.1201/b11499-37

Endsley, M. (1995). Endsley, M.R.: Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors Journal 37(1), 32-64. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*, 32–64. https://doi.org/10.1518/001872095779049543

Fortinet. (2022). *Global Threat Landscape Report A Semiannual Report by FortiGuard Labs—August 2022*. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-1h-2022.pdf

Giles. (1910). *Sun Tzu On The Art Of War* (0 ed.). https://doi.org/10.4324/9781315030081

Gutzwiller, R., Hunt, S., & Lange, D. (2016, March). *Task Analysis toward Characterizing Cyber-Cognitive Situation Awareness (CCSA) in Cyber Defense Analysts*. https://doi.org/10.1109/COGSIMA.2016.7497780

Husák, M., Sadlek, L., Špaček, S., Laštovička, M., Javorník, M., & Komárková, J. (2022). CRUSOE: A toolset for cyber situational awareness and decision support in incident handling. *Computers & Security*, *115*, 102609. https://doi.org/10.1016/j.cose.2022.102609

IBM. (2023). *Cost of a Data Breach Report 2023*.

Kenny, G. (2016). Strategic Plans Are Less Important than Strategic Planning. *Harvard Business Review*, *June 2016*.

Knerler, K., Parker, I., & Zimmerman, C. (2022). *11 Strategies of a World-Class Cybersecurity Operations Center*. MITRE. https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf

Lemay, A., & Leblanc, S. (2018). Iterative Analysis of Competing Hypotheses to Overcome Cognitive Biases in Cyber Decision-Making. *Journal of Information Warfare*, *17*(2). https://www.jstor.org/stable/26633153

Mandiant. (2023). *M-Trends 2023 Special Report*.

Maxwell, A. (1997). Three Levels of War. *USAF College of Aerospace Doctrine, Research and Education (CADRE). Air University Press*, *1*.

Microsoft. (2023). *Microsoft Digital Defense Report 2023*.

NATO. (2021a). *Allied Command Operations Comprehensive Operations Planning Directive Version 3.0*.

NATO. (2021b). *NATO Cyber Defence*. North Atlantic Treaty Organization – Public Diplomacy Division. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf

NATO Cooperative Cyber Defence Centre of Excellence. (2022). *Classified Locked Shields 2022 After Action Reports*.

NATO Cooperative Cyber Defence Centre of Excellence. (2023). *Locked Shields*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/exercises/locked-shields/

Nesbit, P., Kennedy, Q., Alt, J., Fricker, R., Whitaker, L., Yang, J. H., Appleget, J., Huston, J., & Patton, S. (2013). *Understanding Optimal Decision-Making in Wargaming:* Defense Technical Information Center. https://doi.org/10.21236/ADA602079

Osinga, F. (2005). *Science, strategy and war: The strategic theory of John Boyd*. Eburon Academic Publishers.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Pennypacker, J. S., & Cabains-Brewin, J. (2003). *What makes a good project manager*. Center for Business Practices.

Project Management Institute (Ed.). (2021). *A guide to the project management body of knowledge (PMBOK® guide) and the standard for project management* (Seventh Edition). Project Management Institute, Inc.

Schlette, D., Caselli, M., & Pernul, G. (2021). A Comparative Study on Cyber Threat Intelligence: The Security Incident Response Perspective. *IEEE Communications Surveys & Tutorials*, *23*(4), 2525–2556. https://doi.org/10.1109/COMST.2021.3117338

Snowden, D. J., & Boone, M. E. (2007). A Leader's Framework for Decision Making. *Harvard Business Review*, *November 2007*.

Storr, J. (2003). A command philosophy for the information age: The continuing relevance of mission command. *Defence Studies*, *3*(3), 119–129. https://doi.org/10.1080/14702430308405081

Valentine, C. W. M. (2018). *Organizing for Cyber Resilience: Rethinking the Balance Between Prevention*.

Vielberth, M., Menges, F., & Pernul, G. (2019). Human-as-a-security-sensor for harvesting threat intelligence. *Cybersecurity*, *2*(1), 23. https://doi.org/10.1186/s42400-019-0040-0

Williams, B. T. (2014). *The Joint Force Commander's Guide to Cyberspace Operations*.