Demonstration and Evaluation of Defensive Cyber Operations Decision-Making Model

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: As technology has evolved, the world has become more dependent on digital services. Businesses are digitalizing their core processes to better match their clients' needs and critical infrastructure providers are seeking performance improvements from digitalization. When assets are digital, cybercriminals and nation-states are increasing their offensive activities in the cyber domain. As a result of this, cyberattacks are growing in complexity and speed, forcing defenders to advance in their capabilities to respond to these threats. One key element in developing defensive capabilities is to understand the underlying decision-making models providing the basis for more effective tooling, operation planning, and organizational models. The purpose of this paper is to address this need by demonstrating a Defensive Cyber Operations (DCO) decision-making model constructed based on a wargaming exercise, to assess the usability and transferability of the model to real-world cyber operations and to further develop the model based on the feedback received. The research is based on the Design Science Research methodology and focuses on the demonstration and evaluation phases of the selected methodology. The constructed decision-making model was presented to an expert panel, consisting of 17 experienced professionals of 7 nationalities. They were selected based on their known experience of cyber operations or by the recommendation of previously interviewed panel members. The panel contributed to the model with their evaluation and ideas for improvement. Based on the findings of the expert panel, the model was further developed to include a clear notion of escalation for activities requiring a higher mandate, stronger collaboration and reporting with upstream managers and external stakeholders. In addition, several minor improvements were made to improve the usability of the model. The improved DCO decision model presented in this paper is endorsed by the expert panel as applicable and transferable to real-life DCOs, thus laying the groundwork for future research into automation and artificial intelligence augmentation of faster and more accurate DCO decision-making.

Keywords: Decision-Making, Defensive cyber operations, Transferable model, Artificial Intelligence

1. Introduction

Fast technology development speeds up digitalization and makes our societies ever more dependent on digital infrastructure. The number of internet-connected devices is expected to almost double between 2023 and 2030 (Statista, 2024), and cyber risks are seen as the fifth highest category of risk to society due to possible ripple effects caused by cyber incidents (World Economic Forum, 2025b). In addition to the expansion of the attack surface, the increased complexity of the cyber landscape, interconnected operating environments with expanding supply chains, and rapid adaptation of emerging technologies are escalating cyber risks (World Economic Forum, 2025a).

As businesses and assets are becoming more digital, criminals are following. The Federal Bureau of Investigation's Internet Crime Complaint Center reported a 21% increase in Internet crime-related losses in 2023 compared to the previous year (Federal Bureau of Investigation, 2024). Increased geopolitical tension has also increased the number of cyberattacks towards national critical infrastructure (KnowBe4, 2024) creating an urge for both military and civilian organizations to be better defended against cyber threats. In addition, NATO recognizes cyberspace as a domain of operations alongside the traditional domains of air, land, and sea (NATO, 2021).

According to USCYBERCOM (2018), Cyber Operations (CO) can be divided into Offensive Cyber Operations (OCO) projecting power through cyberspace, Defensive Cyber Operations (DCO) preserving the ability to utilize cyberspace capabilities, and Infrastructure Operations preserving confidentiality, availability and integrity of the defended network. DCOs can be further divided into Response Actions (DCO-RA) which are conducted on an external network, and Internal Defense Measures (DCO-IDM) performed inside the defended network. Finnish Defence Forces' adaptation of this model takes into account possible support operations to unknown networks, for example, if a military or cybersecurity services provider is invited to assist another organization during a cyber incident or escalating crisis (Laari et al., 2019). **Figure 1** illustrates a simplified adaptation of different COs and their relations.

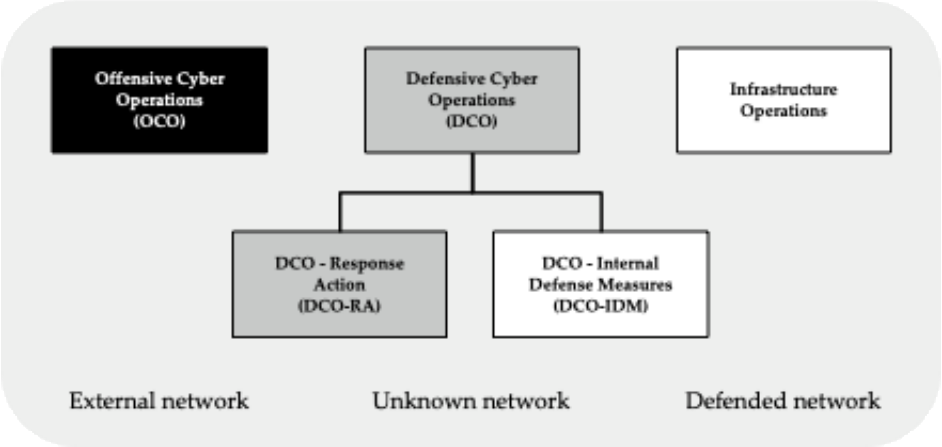

Figure 1: Cyber Operation types based on (Laari et al., 2019; USCYBERCOM, 2018)

Especially with the help of Artificial Intelligence (AI), cyberattacks can be conducted quickly, which requires defenders to speed up their decision-making in order to be effective (Maymí & Thomson, 2018). AI can accelerate COs in a number of ways when human operators learn to cooperate together with AI-based machine operators (Sarjakivi, 2025). Decision-making is one of the capabilities AI can accelerate. According to Cynefin framework, the decision-making approach depends on the context in which decisions are made. In a simple context, the causal relations of actions are relatively straightforward, while in a complicated context, the decision-maker needs to consult an expert to understand the causality. In a complex context, the causality exists but is difficult to identify due to a high number of dependencies and relations, and the decision-maker must rely on experience and capability to make fast corrections. In a chaotic context, causality is non-existent, and the decision-maker must put effort into navigating to any other context rapidly (Snowden & Boone, 2007).

Many decision-making models exist but often they do not take the special requirements of COs into account. One example of a widely used model is the Military Decision-Making Process (MDMP) which relies strongly on thorough planning and clear orders (US Department of the Army, 2020). When combined with the Allied Joint Doctrine for Cyberspace Operations which defines how COs are planned and conducted (NATO, 2020), a trained military person has general tools to perform COs. The issue with this approach is that military models are not always fit for purpose in civilian organizations, and sometimes structured military models can be too extensive and slow for fast-paced COs.

The paper is organized as follows: Section 2 introduces the research methodology, section 3 presents the results of research questions, section 4 introduces the improved decision-making model, and section 5 concludes the study with future research topics.

2. Methodology

2.1 Research Methodology

In essence, the Design Science Research (DSR) methodology had two primary activities: Build and Evaluate (March & Smith, 1995). This research utilizes the extended DSR process introduced by Peffers et al (2006) which, due to its iterative nature, is an especially suitable approach to be used in modern information systems research where the problem and solutions can be relatively complex.

The DSR process shown in **Figure 2** below consists of 6 activities for problem-centric development. The first activity, namely problem identification and motivation, focuses on defining the problem clearly enough so that the definition can be used in solution design. At the same time, the real value of the solution needs to be justified to ensure that the researchers are solving a relevant problem. The second activity, objectives of a solution, defines how success in the process looks like in terms of expected benefits. The third activity, design and development, consists of the creation of an artifactual solution. The fourth activity, demonstration, tests the suitability of the artifacts to solve the defined problem. This can be achieved through experimentation, simulation, a case study, or a similar appropriate activity. The fifth activity, evaluation, assesses if the solution fulfills the expectations set in the second activity or if there is a need to re-iterate the solution by returning to the third activity or even putting more realistic expectations in the second activity. The final activity after passing the evaluation activity is called communication. This activity includes publication of the solution to a wider audience, for example, in the form of a research paper. (Peffers et al., 2006).

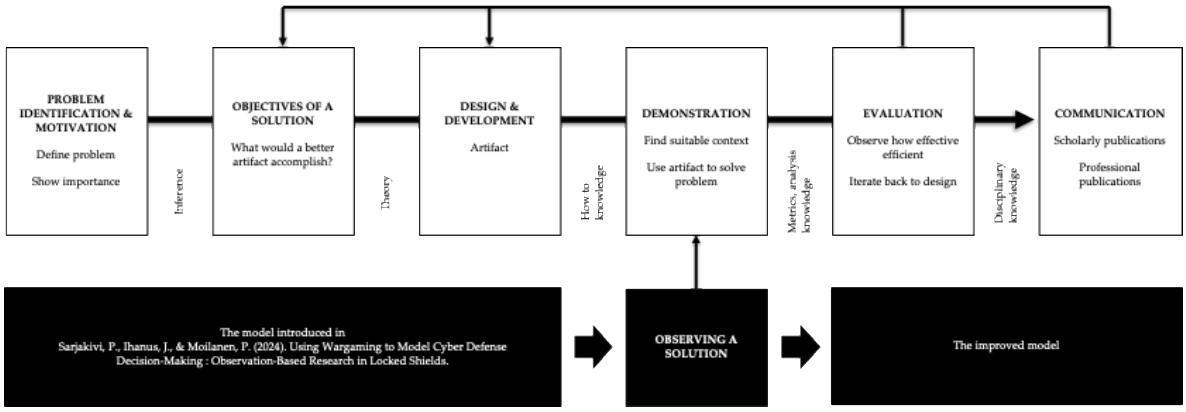

Figure 2: Design Science Research process activities and starting point of this research

As shown in **Figure 2**, this research observes a solution artifact, a decision-making model for DCOs constructed based on the results from a wargaming environment, published earlier by the authors of this research. Consequently, the research focuses on the demonstration and evaluation activities of the DSR process. The objective of this research is to assess and improve the usability and transferability of the model to real-world DCOs. The result of this research is an improved model.

The evaluation method of an artifact depends on the nature of the artifact. According to a framework for selecting methods of evaluation in DSR, the optimal method for evaluation of both the usability and transferability of a model is an expert interview (Müller et al., 2024), which was therefore selected as the evaluation method of this research.

2.2 Observed Solution

The research builds on a DCO leader decision-making model that was constructed after observing leaders of COs during the world's largest live-fire cyber exercise, NATO Locked Shield 2023. The model consists of two distinct processes operating in different Cynefin decision-making contexts and requiring different sets of skills from the leader.

The primary process aims to accomplish the operation within the given boundaries. Typically, it operates in a simple or complicated decision-making context and includes operation planning based on mission order, rehearsing the plan, operations execution, feedback, and after action report. The secondary process initiates when engagement with an active adversary causes unplanned events. It operates typically in complex decision-making contexts and its main goal is to eliminate the impact of unplanned events to continue the execution as planned. DCO leaders must be able to handle both of these processes to accomplish the operation, and deep cybersecurity expertise is needed from DCO leaders at least in the secondary process (Sarjakivi et al., 2024).

2.3 Expert Panel

For this research, 17 experienced professionals were interviewed using a semi-structured interview method. The interviews were conducted in phases in October – December 2024. The initial set of experts was selected based on their reputation and known expertise on this topic. At the end of every interview, the interviewee had the opportunity to recommend experts they believed could contribute to this research. The research plan didn't define an absolute number of interviews, but interviewing was concluded as saturation was reached, i.e. further interviews did not provide any new aspects and expert recommendations started to cycle back to the same persons.

The structure of the expert panel was as follows:

- 17 experts represented 7 different countries from different national leadership cultures. This is aligned with Hofstede & Hofstede's definition (Hofstede & Hofstede, 2010) for different countries and their typical leadership cultures.
- 70% (12) of experts had previous experience from the exact same wargame (exercise) the modeling was based on, namely NATO Locked Shields, which is the largest cyber defense exercise in the world. In addition to the experience of real-life DCO, this overall experience helped the experts to validate whether the model was correct in the context in which it was created, and what the key differences were between this wargame and real life.

- 59% (10) of experts had the experience of leading their nation's blue team, most with top-ranking results. With this experience, they have had to think about decision-making structures in similar DCOs.
- 47% (8) of experts were currently military officers and an additional 47% (8) had been working in a military context as reservists, contractors, or are ex-officers. This diversifying background contributes to the understanding of different contexts of DCO decision-making.

Together with the interview invitation the interviewees received the article describing the constructed model and questions to be asked in the interview. Each expert was interviewed independently using an online meeting tool and expert results of open and closed questions were recorded.

2.4 Research Questions

This research aims to answer the following questions:

RQ1: Is the constructed model valid?

RQ2: Is the model usable and transferable to real-life DCO context?

RQ3: What are the most critical decisions a DCO leader must make?

RQ4: What are the potential applications of AI in enhancing decision-making processes and optimizing COs?

3. Results of Research Questions

3.1 RQ1: Is the Constructed Model Valid?

The first research questions focused on verifying the validity of the constructed model within the operating environment in which it was constructed. *All 17 expert panel members confirmed the model's validity*, some with the changes implemented into the improved decision-making model demonstrated in section 4.

24% of expert panel members (4) commented about the model's similarities, or even overlapping nature with standard military processes in their countries, for example, the Military Decision-Making Process (MDMP). These processes are built for generic military purposes and can be utilized in COs if the organization has the right skill set and experience from the process, and the whole organization utilizes them. For organizations that are not utilizing processes like MDMP, such as civilian organizations and non-military public organizations, this model provides a streamlined version process for COs. Additionally, if only 4 out of 16 persons with military experience commented about the overlap, the suitability of current military processes is not obvious.

3.2 RQ2: Is the Model Usable and Transferable to Real-Life DCO Context?

The second research question aimed to understand if the model constructed for the wargaming environment is transferable to real-life DCOs and therefore usable outside the environment in which it was created. As shown in **Figure 3**, *all 16 experts responding to this question confirmed the model's transferability to real-life DCOs,* some with the changes implemented into the improved decision-making model demonstrated in section 4. Half of the responders believed that the model could be used in most real-life DCOs, while the other half specified a certain use case, namely threat hunting, Digital Forensics and Incident Response (DFIR), or cybersecurity, where the model would be usable.

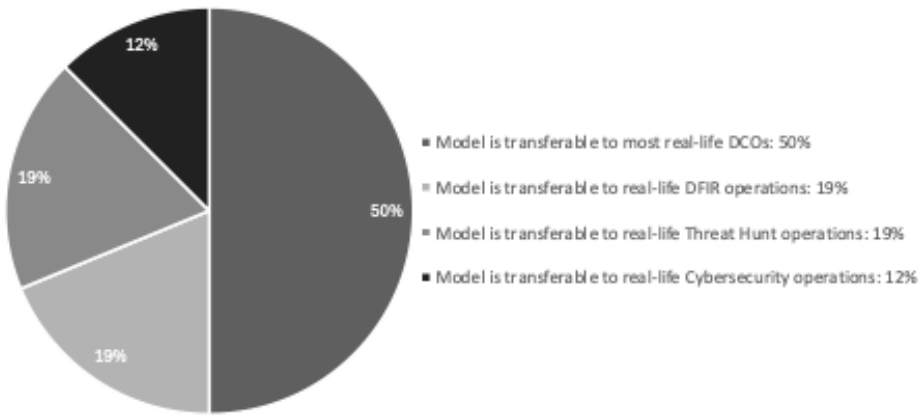

Figure 3: The model's transferability to real-life DCO

Of the experts, 29% (5), commented that the wargame, NATO Locked Shields, in which the model was constructed, did not provide a good reflection of the DCOs in real life. At the same time, all the experts commenting on the real-life correspondence of the wargame setup agreed that it was the most comprehensive of the COs that researchers can observe and publish research on. The main problem is its isolated nature, where blue teams perform operations independently to asset owners and their operators' assistance with an extensive mandate to for example keep the whole region out of the electricity for extensive periods of time. This renders the exercise to be more of an administration exercise than a CO. Another problem mentioned was the open definition of the desired end state for the protected environment, where in real-life operations the end-state would be something that can be handed over to the infrastructure operations team which works with standardized tools and procedures.

3.3 RQ3: What are the most critical decisions a DCO leader must make?

The third research question aimed to improve the implementation of the decision-making model by defining priority decisions. Every expert panel member was asked what concrete decisions the DCO leader needs to make and on what data points the decision is based. The responses were clustered into seven categories shown in Table 1. The table indicates also the process within the decision-making model where the decision is typically taken.

Table 1: The most important decision a DCO leader needs to make

Decision	Experts referred	Process where decided
Prioritization of defended capabilities and assets	9	Primary
The right resourcing and allocations	9	Primary, Secondary
Proper response	9	Secondary
When to report upstream leaders	6	Secondary, Primary
If a higher mandate is needed	5	Secondary
When to intervene in a subordinate's actions	4	Primary, Secondary
The right timing for execution	2	Secondary, Primary

Prioritization of capabilities to be defended and assets is one of the most important decisions leaders must make. This decision steers the team's work towards maximizing the value of the work. With clear communication of the priorities, the team is more aligned and capable of making the right decision low in the hierarchy (US Department of the Army, 2019). The decision of the right resourcing and allocations was identified as equally important. With properly allocated effort, the power can be concentrated on critical points. Additionally, the leader must be able to oversee the operation execution and decide when and how to intervene in a subordinate's actions, in case the operation needs steering.

The third decision category ranking high in expert panel results was deciding a proper response to adversary actions in the secondary process. This links to decisions about when the reporting threshold or current mandate is exceeded. Leaders must consider if and what kind of support is needed, or what are the consequences to frame operation if the plan needs to be changed. Also, the right timing to execute counteractions is an important decision that can help the defender gain the element of surprise by taking the initiative (US Department of the Army, 2019).

According to the expert panel, these decisions are based on the following information, serving different purposes:

- Understanding of the operational environment gained through Cyber Situational Awareness (CSA) and Cyber Threat Intelligence (CTI). This information helps to understand the likelihood or probability of an event to happen.
- Impact analysis conducted for identified or estimated adversary action helps to understand the consequence of an event.
- Benchmarking against decisions made in the past. This information can be used to validate, justify, or reason the decision.

For example, a DCO leader can utilize the formula of *consequence * likelihood* to evaluate the size of the risk (British Standards Institution, 2022) and choose the right priority for risk mitigation. The decision made can be then benchmarked against the decision taken earlier to gain confidence in the decision.

It's noteworthy that 24% (4) of the experts believed that strong cybersecurity knowledge is essential for DCO leaders to make these critical decisions in both primary and secondary processes. The original model defined deep cybersecurity knowledge as a mandatory skill for DCO leaders in the secondary process due to its high tempo and complex Cynefin context but expected that DCO leaders have enough time to consult trusted experts in the primary process. Eventually, the needed depth of DCO leaders' cybersecurity knowledge in the primary process depends on team dynamics and the operation they are performing.

3.4 RQ4: What are the Potential Applications of AI in Enhancing Decision-Making Processes and Optimizing COs?

According to a recent Systematic Literature Review (SLR), there are at least 22 use cases for AI to accelerate COs (Sarjakivi, 2025). This research question aimed to identify the most relevant use cases from the expert panel's point of view. **Table 2** demonstrates 14 use cases identified by the expert panel, together with occurrences the expert panel referred to them. The third column indicates the reference amounts adjusted with SLR's source articles amounts. The closer these values are to each other the more aligned these studies are.

Table 2: AI use cases accelerating COs

Use case	Experts referred	SLR -adjusted
Information sharing and reporting	10	7.65
Data fusion, enrichment, and visualization	10	3.28
Course of Action (COA) recommendation	8	3.06
Anomaly detection	5	1.27
Document summarization and data scraping	4	9.18
Code, script, query, and rule generation	3	3.44
Performance management and workload balancing	3	1.38
Threat intelligence	2	0.76
Action log documentation	2	2.29
Target and response validation	2	0.51
Vulnerability management	1	1.15
Attack surface analysis	1	0.33
Training users and systems	1	0.76
Detect must-win battles	1	-

Interviewed experts highlighted Large Language Model (LLM) related capabilities, like information sharing and reporting, data fusion, enrichment and visualization, Course of Action (COA) recommendation, and document summarization and data scraping. The targeted benefits of these capabilities are primarily focused on time-saving in data processing, such as changing the format or adding contextual information, improved analysis when all relevant data is available for decision-making, and faster decision-making with the assistance of AI. Some of these use cases were not encountered as frequently in the compared SLR research, as LLMs are relatively new technology. The expert panel identified a new use case that SLR research didn't recognize, namely the detection of must-win battles. In this use case, AI can help CO leaders identify critical points where operations must be successful, assist leaders in identifying these must-win battles, and guide them through these situations.

4. Improved DCO Decision-Making Model

The section focuses on highlighting the changes and improvements in the model, while the original article (Sarjakivi et al., 2024) provides a more thorough introduction to the model.

4.1 Improvements

In total, the expert panel provided 61 comments to the model, which is on average 3,6 comments per expert. Those comments were clustered into 17 improvement ideas. Some of the ideas contradict each other. For example, 47% (8) of panelists emphasized the role of thorough planning, while 18% (3) of experts claimed that in DCO there is not enough time to plan actions thoroughly enough and the model should be streamlined for time-sensitive operations. One expert proposed that the secondary process is not needed at all, as the planning

in the primary process eliminates unplanned events, while most of the experts saw the need and even 18% (3) of experts believed that the planning phase should define threshold limits to enter the secondary process. Similarly, for both requests for more mandates (5 experts against 1 expert) and the increased role of CTI in planning (5 experts against 1 expert), the results comments were contradicting. As a result, 3 major changes were made to improve the model.

4.1.1 The increased role of operation planning

47% (8) of the experts highlighted the role of thorough operation planning to avoid entering the secondary process. The planning process should include the identification of different COAs and the creation of alternative plans for different scenarios. Plans should be challenged or "war gamed" with relevant experts to find the weak spots in the plans (Wade, 2023). 29% (5) of experts reminded that CTI is a natural part of operations planning, and in addition to planning for counteraction to adversary COA, battlespace should be prepared by setting traps and early warning mechanisms. Operation planning should utilize the lessons learned from previous operations (12% (2) of experts) and build on pre-existing toolsets, playbooks, and procedures (24% (4) of experts) to make the plans easier to implement. Standardization and pre-made plans help when there is not enough time for proper planning and testing, which is often the case with DFIR cases. Also, the handover of the results of the operation, for example, network hardening, is easier when the tools and procedures are standard and interoperable with the receiver. As are result of expert comments, the primary process is strongly linked with a readiness to conduct operations.

4.1.2 Visible stakeholder communications

35% (6) of the experts noted that communication with both internal and external stakeholders is not visible enough in the model. In addition to mandatory reporting, stakeholder communications can be utilized for expectation management and preparing stakeholders for upcoming resource requests. Also, the unbalance between fast-phased events in cyberspace and the human decision-making cycle, especially when external parties are involved, needs proactive communications. 29% (5) of experts mentioned that communicating with stakeholders might be necessary to verify the given mandate in unclear situations or ask for a higher mandate. According to experts, stakeholders often lack an understanding of cyberspace and therefore the DCO leader must be able to communicate in stakeholders' terms and with concrete descriptions of potential effects. In addition to cyber knowledge, culture, attitude, other priorities, and the possibility of getting involved can affect stakeholders' readiness to communicate at the right time with the DCO leader. 18% (3) of experts identified proper stakeholder communication as a method to ensure the interoperability with frame mission.

4.1.3 Changes in the operation and mandate during execution

24% (4) of experts reminded that DCO leaders must be prepared for changes in operations. COs typically support larger frame operations and are therefore subject to change due to external reasons. The complex nature of cyber incidents and the ever-changing cyber threat landscape contribute to the unpredictability of operations. This notion affected both primary and secondary decision-making processes.

4.2 The DCO Decision-Making Model

The improved decision-making model is presented in **Figure 4**. This improved version's terminology is aligned with NATO AJP 3-20 and MDMP, and the model recognizes better the stakeholders and changing order from frame operation.

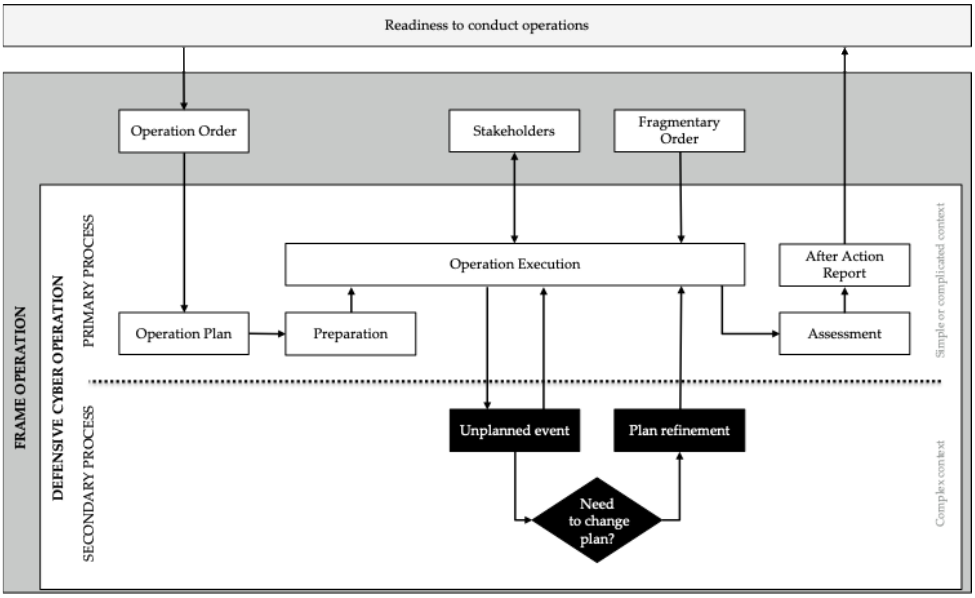

Figure 4: Improved version of two distinct decision-making processes in the defensive cyber operation

The primary process aims to accomplish the operation according to the plan and is initiated by an operation order received from the frame operation. Operation order defines the objectives for the operation together with resource and time constraints. The civilian equivalent for frame operation is typically the business operation of the defended target and operation order is the contract made between for example DFIR service provider and client company fallen victim to breach.

Operation planning is based on operation order requirements and the team's readiness to conduct operations. After the plan is approved, the team prepares for operation execution by setting up the required capabilities and rehearsing the plan. During the operations, the team executes tasks in the order defined in the plan, while communicating with internal and external stakeholders to ensure the alignment with frame operation. After the execution, the team assesses the operation and produces after action report with lessons learned to support the future readiness to conduct operations.

The secondary process is initiated when an active adversary engagement causes an unplanned event in the primary process. The secondary process presented in detail in **Figure 5**, aims to minimize unplanned event's impact on operations plan execution. Decision-making in the secondary process is based on CSA observing its own mission status, CTI observing the adversary's operation, and possibly changing mandate from frame operation. In DCO-IDM the actions are performed towards its own operational environment while in OCO and DCO-RA the power can be projected towards the adversary's operational environment.

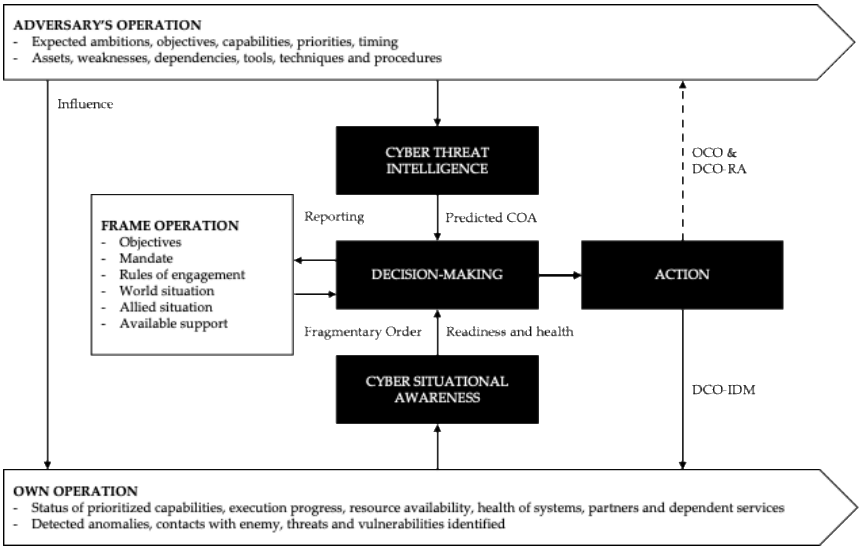

Figure 5: Dynamic decision-making in the improved secondary process

5. Conclusion

While digitalization increases rapidly, organizations and nation-states must improve their capabilities to defend digital infrastructure from cyber threats. Although traditional national defense remains the responsibility of militaries and other security authorities, digital defense must be done with civilian organizations, as they own and operate most of the digital infrastructure and underlying assets (Azrilyant et al., 2022). Therefore, the art of COs must be known by both entities.

Based on the evaluation of 17 experts, the constructed model was verified to be valid for the operating environments in which it was created and was seen as usable and transferable to real DCOs. The prioritization of defended capabilities and assets, the right resources and allocations, and the right response were seen as the most important decisions DCO leaders must make during operations. AI was seen as particularly capable of assisting with information sharing and reporting, data fusion, enrichment and visualization, and COA recommendations.

Based on the results of this study, a refined decision model was constructed. The model can be used as a basis for further research into decision-making and the acceleration of DCOs, for example using AI. In addition, this research, together with the original paper defining the model construction, can support the familiarization of DCO leaders with NATO Locked Shields and provide improvement ideas for the exercise organizers.

For future studies, the possibility of using AI to accelerate decision-making in DCOs is the most prominent research topic. In particular, the key decisions mapped during the interviews and presented in **Table 1** provide an excellent starting point for possible AI implementations. Additionally, using this decision model could be supported with implementation guidelines and further research within specific operating environments. Regardless of the methodology utilized in this research, there is always a risk of subjectivity, and therefore the true benefit of the model can only be recognized by verifying the implemented model in a suitable operating environment.

Acknowledgements

The authors would like to thank Business Finland for supporting the writing of this article (grant number 671/31/2022).

References

Azrilyant, J., Sidun, M., & Dolashvili, M. (2022). Fact and Fiction: Demystifying the Myth of the 85%. The George Washington University Elliott School of International Affairs.

British Standards Institution. (2022). ISO 31073—Vocabulary for risk management about. BSI.

Federal Bureau of Investigation. (2024). Internet crime report 2023.

Hofstede, G., & Hofstede, G. J. (2010). Cultures and organizations: Software of the mind. McGraw-Hill.

KnowBe4. (2024). Cyber Attacks on Infrastructure: The New Geopolitical Weapon. https://www.knowbe4.com/hubfs/Global-Infrastructure-Report-2024_EN_US.pdf

Laari, T., Flyktman, J., Härmä, K., Timonen, J., & Tuovinen, J. (2019). #kyberpuolustus: Kyberkäsikirja Puolustusvoimien henkilöstölle. Maanpuolustuskorkeakoulu.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. Decision Support Systems, 15(4), 251–266. https://doi.org/10.1016/0167-9236(94)00041-2

Maymí, F. J., & Thomson, R. (2018). Human-Machine Teaming and Cyberspace. In D. D. Schmorrow & C. M. Fidopiastis (Eds.), Augmented Cognition: Intelligent Technologies (Vol. 10915, pp. 299–315). Springer International Publishing. https://doi.org/10.1007/978-3-319-91470-1_25

Müller, J., Würth, S., Schäffer, T., & Leyh, C. (2024). Toward a Framework for Determining Methods of Evaluation in Design Science Research. 231–236. https://doi.org/10.15439/2024F7208

NATO. (2020). Allied Joint Doctrine for Cyberspace Operations (AJP-3.20).

NATO. (2021). 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

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., & Hui, W. (2006). The Design Science Research Process: A Model For Producing And Presenting Information Systems Research. Proceedings of 1st International Conference, DESRIST 2006, 83–106.

Sarjakivi, P. (2025). Artificial Intelligence Accelerated Cyber Operations: A Systematic Literature Review. Journal of Information Warfare, 24(1).

Sarjakivi, P., Ihanus, J., & Moilanen, P. (2024). Using Wargaming to Model Cyber Defense Decision-Making: Observation-Based Research in Locked Shields. European Conference on Cyber Warfare and Security, 23(1), 457–464. https://doi.org/10.34190/eccws.23.1.2270

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

Statista. (2024, July). IoT connections worldwide 2022-2033. Statista. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

US Department of the Army. (2019). Army Doctrine Publication 6-0. Mission Command: Command and Control of Army Forces. Washington, DC. https://apps.dtic.mil/sti/trecms/pdf/AD1158686.pdf

US Department of the Army. (2020). Army Techniques Publication 5-0.2-1. Staff Reference Guide Volume I Unclassified Resources. Washington, DC. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN34870-ATP_5-0.2-1-000-WEB-1.pdf

USCYBERCOM. (2018). Joint Publication 3-12 Cyberspace Operations. United States Joint Chiefs of Staff.

Wade, N. M. (2023). BSS7: The Battle Staff SMARTbook (7th ed.). The Lightning Press.

World Economic Forum. (2025a). Global Cybersecurity Outlook 2025. https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

World Economic Forum. (2025b). The Global Risks Report 2025. 20th Edition. https://www.weforum.org/publications/global-risks-report-2025/