Officers' Perceptions on Cyberwarfare Enhanced with Artificial Intelligence

Maija Turunen and Maria Keinonen
Finnish National Defence University, Helsinki, Finland

maija.turunen@yahoo.com
maria.keinonen@mil.fi

Abstract: The use of artificial intelligence (AI) in both cyberwarfare and conventional warfare is increasing, as is the debate over its ethical acceptability. At the same time, technological development is shaping our perceptions of the character of war. Military decision-makers play a central role in the development and employment of artificial intelligence and cyber power in warfighting. To understand the ethical considerations surrounding the use of these emerging technologies, it is vital to examine military decision-makers' perceptions of the topic. This paper presents the results of surveys conducted among students of the Finnish General Staff Officer Course in 2023 and 2025. The surveys specifically aimed to evaluate officers' attitudes toward the acceptability of employing artificial intelligence and developing cyber warfare capabilities within military operations. The study sought to clarify how officers conceptualise these topics within military thinking and how this understanding shapes future cyber warfare. The main results indicate that officers strongly support using artificial intelligence for demanding military tasks, provided human involvement in decision-making (Human-on-the-Loop) is retained. Respondents were sharply divided on the likelihood of war occurring solely in cyberspace in the near future. Overall, military necessity remains the main consideration shaping attitudes toward AI's military use.

Keywords: Cyberwarfare, Artificial intelligence, Character of war, General staff officer Perceptions, Military AI

1. Introduction

The use of artificial intelligence in various weapons systems, both conventional and cyber, is becoming more common. AI offers numerous possibilities for military use, but its effective implementation requires, among other resources, a new kind of military thought, the development of new operational concepts, processes and tactics, a reassessment of security threats and the identification of ethical and legal issues. The capabilities created by AI can also shape the understanding of warfare. According to Johnson (2021, 2), AI technologies can affect future warfare and international security in three interrelated ways: 1) by increasing the uncertainty and risk posed by existing threats (both physical and virtual); 2) by changing the nature and characteristics of threats; and 3) by introducing new threats into the security environment.

In addition to training and experience, military leaders' own military thought and professional ethics influence their understanding of the character of warfare, i.e., how, when, where, and with what kind of military methods an external armed attack or threat should be responded to. Military leaders are also responsible for developing operational art and military capabilities and for their use.

Despite the essential role of officers in developing and utilising AI-enabled conventional and cyber warfare methods, and their attitudes towards new technologies, there is little public research on the subject. In the United States, Peter Lushenko (2024) conducted a 2023 study on the trust of those serving at the Carlisle and Newport military academies in working with AI-enhanced military technologies. In Australia, researchers from the University of New South Wales studied in 2019 the attitudes of Australian Defence Force Academy cadets towards interaction with autonomous weapon systems (Galliott & Wyatt, 2022).

The main research question in this study was: "How do officers notice the possibilities and limitations of cyber warfare methods and AI in modern warfare?" The question sought to determine whether these factors have been instrumentalised in officers' thought as elements of warfare and, more broadly, as factors shaping the character of war. The study was a survey that used both quantitative and qualitative questions to examine the views of General Staff Officer Course students on the topic.

Constructive war theory provided a theoretical framework for structuring the research question. This research explores shared understandings of AI and cyber methods as threats that must be responded to, but also as tools that can be used to project power.

2. Theoretical Background

This research is based on the application of the constructive theory of character of war. In a constructive theoretical framework, the character of war can be defined as follows: the character of war refers to the common perceptions in the international system about the nature, needs, and possibilities of the use of armed

forces, as well as the effective principles and operational models of armed forces. In the theory of character of war, war was viewed as a pragmatic and changing phenomenon. The war character is embedded in the international system and security environment, as well as in operational logic, strategic communication, rules, and the influence of new technological advances. It also establishes an association with the actors' identities. Through the character of war, the creator of the character of war seeks to outline the prevailing military threats against which one must be able to wage war; the situation in which war may be waged; the methods by which war is to be fought; the factors that can be used to increase credible military power; and the objectives of warfare. (Raitasalo and Sipilä, 2008; Vego, 2011).

On a broader scale, the character of war and its formation involves, in addition to military factors, various levels of diplomatic, political, economic, social, ethical, cultural, informational, technological, and legislative elements. Tähtinen (2024) describes this as the external nature of war, which embodies the changing manifestation of war in the outside world.

The technical development has introduced new dilemmas in defining the character of war, especially from a cyberspace perspective, where artificial intelligence is a powerful driver of change. The evolution of military cyber capabilities has brought the definition of war into transition. Hybrid warfare, which includes the use of cyber capabilities, has blurred the line between war and peace. Defining war remains essential, as warfare involves the use of state military power, which—according to Western perspectives—requires a legitimate legal basis. The concept of security is also linked to war and the insecurity it generates (Vilander et al., 2019). Consequently, conflicts in the cyber domain inevitably entail ethical considerations.

The existence and definition of “cyberwar” remain debated. Some scholars argue that the term “war” should not be applied in this context, as it stretches the definition excessively and risks conceptual inflation (Cepik et al., 2015). Others define cyberwar as “state-led attacks on another state’s cyber environment, intended to cause disruption or damage to networks or connected devices” (Clarke & Knake, 2010, p. 109). Drawing on Clausewitzian principles, three criteria must be met for an activity to constitute war: (1) it must have destructive effects, (2) it must target the critical elements of the state, and (3) it must serve political objectives (Cepik et al., 2015). From this perspective, cyberwar can be understood as a state-conducted offensive that targets an adversary’s cyber domain, causes a destructive impact on its critical infrastructure, and influences its political decision-making.

In contrast to “cyberwar”, the term “cyber warfare” is a more straightforward concept. In academic literature, it is often placed alongside other traditional domains of warfare, such as naval or aerial warfare. Linguistically, cyber warfare can be seen less ambiguous than cyberwar, as the former refers to the act of fighting rather than the entire conflict (Lehto & Limnell, 2017). Cyber warfare differs from traditional warfare in that cyber-attacks can directly harm civilian society below the threshold of war (Mazarr et al., 2022). Moreover, in the physical domain, the threshold of war is more clearly defined, whereas in cyberspace, offensive and defensive operations occur continuously without a clear link to declared hostilities (Lehto & Limnell, 2017).

Although the understanding of the nature and goals of war has remained the same throughout the centuries, theories related to warfare are always a product of their time (Vego, 2011). When defining the character of war, the distinct and unconventional nature of the cyber domain must therefore be considered. Within this context, cyber warfare is warfare conducted within or through cyberspace.

3. Methodology

The empirical part of the study consisted of a survey administered to students in the General Staff Officer (GSO) courses of the Finnish Defence Forces (FDF) between 2023 and 2025. The object of the survey was to get an understanding of officers´ perceptions of artificial intelligence and cyber warfare by surveying students' opinions on the subject.

The respondents were selected for their professional military experience. The respondent population (N=134) consisted of officers from all branches of the FDF and the Border Guard. This can be considered a comprehensive sample, considering the number of officers of a similar level who have served in the FDF for a similar period of time, from ten to fifteen years.

Answers were gathered via the open-source learning platform Moodle, including both structured and open-ended questions. Answers to structured questions were analysed using Excel. For each option, respondents were offered a Likert-type scale with five options: 1 = Fully disagree, value 2 = Somewhat disagree, value 3 = Neither agree nor disagree, value 4 = Somewhat agree, value 5 = Fully agree. After each structured question, respondents

were given the option to elaborate on their answers with open-ended questions. These answers were analysed using inductive content analysis (Puusa et al., 2020). The structured questions were obligatory using the given scale, and the open-ended questions were voluntary, with no limitations on answer length.

Likert-type data contains separate items that are not intended to be combined in the analysis, unlike the original Likert scale. Despite this, the Likert-type scale can utilise similar features to the original version, for example, response alternatives. (Boone & Boone, 2012) Since this study examined respondents' views on different types of topics, between which no correlation had been established, a Likert-type scale was best suited for the survey. The frequency of responses was calculated to determine the number of distinct observation types in the data (Heikkilä, 2004).

Approximately 68 per cent of respondents provided open-ended answers. The answers were analysed using inductive content analysis, which allows the researcher to identify similarities, differences, and recurring themes in the material. These findings can then be organised into categories to simplify the main findings from the data (Saunders et al., 2012).

During the content analysis, repeating themes were identified and grouped into categories. This process identified key points in the open-ended responses that helped explain the variation observed in the structured questions. After analysing the quantitative and qualitative data separately, the results were compared to gain a broader understanding of the topic.

The reliability of a survey can be assessed by examining the sample size, the chosen population, the response rate, the consistency of responses, and potential measurement errors (Hirsjärvi et al., 2005). A total of 134 individuals responded to the survey, representing 69 per cent of those invited to participate. The sample size can therefore be regarded as representative of the target group. The participants were officers from different backgrounds, so the chosen population and the results reflect a military perspective. Each phenomenon was assessed using single-item measures, and no correlations were mathematically calculated. This design introduces the potential for measurement error or respondents' misinterpretation of questions. However, an examination of the open-ended responses indicated no evidence of such misunderstandings. Measurement errors were further minimised by maintaining consistent wording and applying the same response scale across all survey items.

4. Survey Results

The aim of the survey was to determine officers' views on the acceptability and trust in the use of AI, as well as on the development of cyber capabilities. The aim of the study was to understand the potential impacts of the above-mentioned topics on the character of future warfare, the functions of military organisations, and military culture. The questions assumed that there was no legal obstacle to the statement and that a similar solution had been approved in other NATO member states.

The following statements were investigated in the survey with a question “Do you agree or disagree with the following statement?”:

Statement 1: Advanced artificial intelligence could independently manage precisely defined and limited military operations, including giving orders to soldiers.

- Statement 2: The use of artificial intelligence should be limited to routine data collection and monitoring tasks.
- Statement 3: I could directly rely on the common operational picture generated by an AI system in multi-domain operations.
- Statement 4: Cyber and electronic warfare capabilities have significantly changed the formation of the character of war.
- Statement 5: Cyber operations should be refrained from if their consequences are not precisely known.
- Statement 6: war solely in cyberspace is possible in the near future.

Regarding the first statement, “Advanced artificial intelligence could independently manage precisely defined and limited military operations, including giving orders to soldiers”, the following themes were discernible from the responses: human responsibility and decision-making must be preserved, artificial intelligence as a support for decision-making and planning, and technical and ethical uncertainty. The results are visualised in Figure 1.

Many respondents emphasise that artificial intelligence cannot and should not make decisions for humans, especially decisions that have an impact on human lives, the use of lethal force, or legal liability. Several respondents also added an ethical and criminal justification to this and emphasised that responsibility for the use of lethal force should always lie with a human. This theme also partly includes the "human in the loop" thinking: artificial intelligence can support decision-making, but humans should always have the last word. On the other hand, situations were identified in which an order is needed to carry out an action for which there is practically no alternative, in which case AI could issue an order just as well as a human. It was also suggested that AI could give orders to autonomous systems, but not to humans.

Another strong theme is viewing AI as an effective tool for planning, analysis, and preparation. The usefulness of AI for giving orders was justified, among other things, by its rationality, efficiency and speed. Respondents consider it realistic that AI can produce command structures, create a situational picture, model options and risks, and act as a decision support system.

The third theme concerns the maturity of the technology and its ethical issues. According to respondents, current AI is not "sufficiently developed", but in the future, its role may increase in limited tasks. At the same time, many find it difficult to define the boundaries because "strictly limited" is an ambiguous term, and liability issues will only be resolved as development progresses.

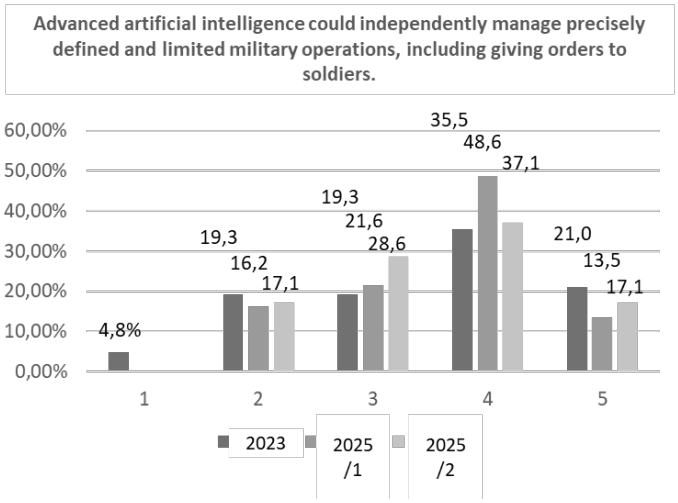

Figure 1: Answers to the question 1

The following themes emerged from the responses to the second statement: "The use of artificial intelligence should be limited to routine data collection and monitoring tasks". The use of artificial intelligence should not be narrowly limited in advance; possibilities for development should be secured, and it should be used as a support for decision-making and in broader military tasks. The results are presented in Figure 2.

Several respondents mentioned that limiting artificial intelligence to routine data collection and monitoring would be harmful and a deliberate weakening of one's own performance. Limits should be set on a case-by-case basis based on reliability, security and usability – not on categorical "only for routine tasks" policies. Respondents also argue that AI should be used much more broadly than just for data collection, especially for decision-making support and certain combat-related tasks, while ensuring humans retain responsibility and are "in the loop."

Responses in favour of limitations highlighted the current state of AI and human ability for innovative, multidimensional thought. Ethical and moral requirements emerged in the responsible development and use of AI. In the results of the autumn of 2025, a significant change occurred regarding this question, which was also strongly reflected in the verbal justifications of the responses. The majority of responses considered that AI should be utilised to its full extent and used as widely as possible. Such limitations would only transfer the advantage to the adversary. Not all actors are as rational as Western countries and will also develop and use AI for other military applications.

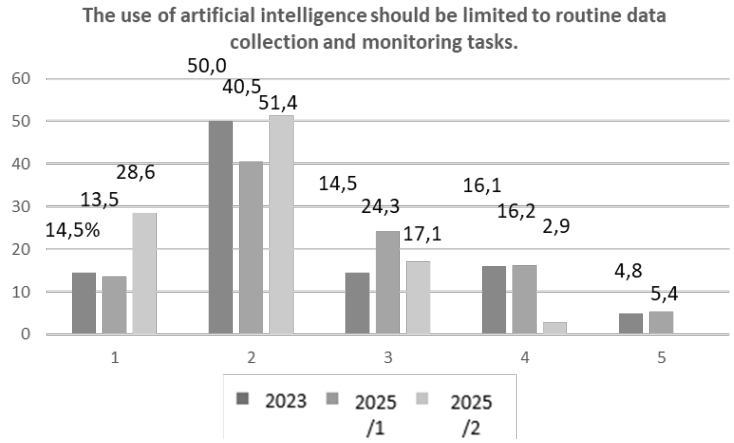

Figure 2: Answers to the question 2

Three main themes recurred in the responses for the third statement, "I could directly rely on the common operational picture generated by an AI system in multi-domain operations.": 1) trust in the AI generating common operational picture (COP) is possible if the system is sufficiently tested and known; 2) the AI generated COP is good and often better than made by a human, but a human is wanted to be involved in the interpretation; 3) trust for AI in this context is currently limited, but could increase in the future. The results are shown in Figure 3.

Many respondents mentioned that they can only trust the COP produced by artificial intelligence if certain conditions are met: the system has been sufficiently tested, its reliability has been demonstrated in practice, and its operating logic is understandable. Some of the respondents emphasised that AI can combine vast amounts of data, make fewer mistakes than a single human, and is particularly good in complex multidomain environments.

Many respondents clearly distinguish between the present and the future. This group does not rule out trusting the AI-generated COP, but clearly positions itself on the "not yet completely" axis. Also, many responses emphasised the importance of humans as final analysts and decision-makers, but the need to fight other AI was also mentioned.

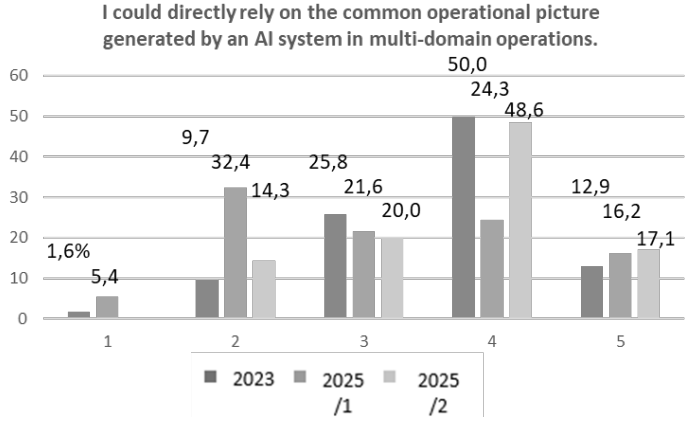

Figure 3: Answers to the question 3

In the numerical responses to the fourth statement, "Cyber and electronic warfare capabilities have significantly changed the formation of the character of war," the majority of respondents supported the statement, but their significance in changing the character of war was divided, based on open-ended responses. The results are illustrated in Figure 4.

In the open-ended responses supporting the claim, it was assessed that cyber performance has significantly changed the character of war because various systems and data transfer are central to maintaining the tempo of operations, where protection, intelligence, and effective impact are essential factors in mission assurance. It was also assessed that the character of war has become increasingly technological in other ways.

The respondents who did not support the claim noted that the war in Ukraine demonstrates the continued centrality of traditional kinetic warfare, such as territorial conquest and the use of kinetic capabilities. Electronic warfare was seen as a more concrete influencer than cyber, especially through the exploitation of the electromagnetic spectrum. According to some respondents, the changes have focused more on the control and use of the battlespace and have broadened the understanding of the diversity of warfare. It was also assessed that these capabilities have contributed to blurring the grey area between war and peace.

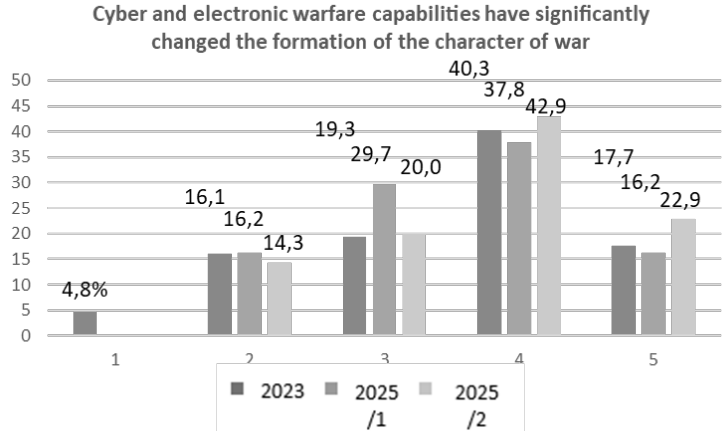

Figure 4: Answers to the question 4

Three main themes recurred in the responses for the fifth statement "Cyber operations should be refrained from if their consequences are not precisely known": 1) there exist the same principles of risk assessment as in kinetic operations, 2) cyber represents a softer means, and 3) the realities of war require risks in certain situations.

The uncertainty of the consequences of cyber operations was evident in responses along the same lines as for other military actions: there is no such thing as complete certainty in advance, but risks must be assessed. Some of the respondents equate cyber operations with other military operations: the consequences are not fully known anywhere (for example, kinetic warfare in general, artillery, nuclear weapons), so positive identification, collateral damage estimation and risk assessment are sufficient as they are now. Cyber was seen as a less violent means to be used before kinetic force, but a secondary impact analysis (concerning bystanders, society, and infrastructure) is still needed. The decision depends on the situation: in existential defence of a state, risks are taken even when information is lacking; in offensive, more cautiously.

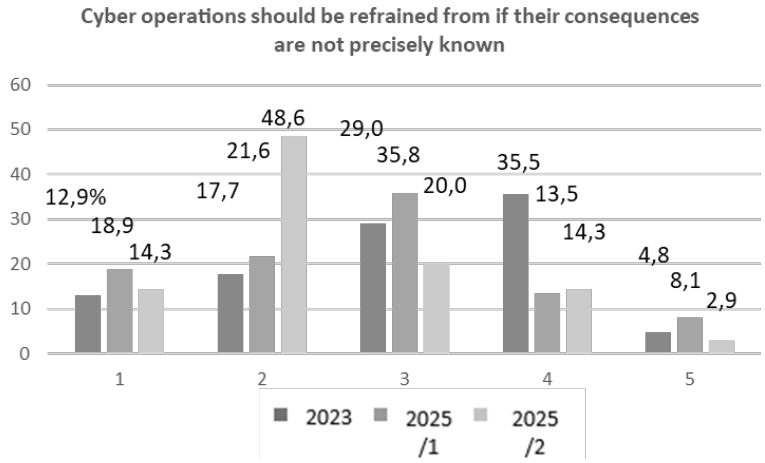

Figure 5: Answers to the question 5

The results for the sixth statement, "A war solely in cyberspace is possible in the near future," are presented in Figure 6. A war solely in cyberspace is seen as theoretically possible but unlikely in the near future. The three most recurring themes are: the inability of cyberwar to achieve strategic goals; escalation into other domains; and the role of cyber as part of a total war, not as an independent one. The largest group believes that cyber operations alone do not force an adversary to do what they want: one cannot conquer territories, kill people, or resolve conflicts without kinetic force. The conflict does not remain in cyberspace: it either expands into kinetic

warfare or fails to meet the criteria of "war". Cyber operations are already underway "below the threshold of war", but do not constitute an independent war - it is a question of definition.

The majority of respondents argued that warfare in a single domain alone is not possible. On the other hand, other respondents believed that some conflicts between states could be resolved solely through cyber warfare, but if the intention is to subjugate another state to one's will or destroy another nation, then conventional warfare is required. Some respondents believed that war is already being waged in the cyber domain all the time, but this does not necessarily escalate in other domains, due to, for example, the attribution problem. The term “war” received a mixed reception, both for and against. Some respondents believed that cyberwar is not war at all, while others saw it as a form of warfare or a question of defining the concept of war.

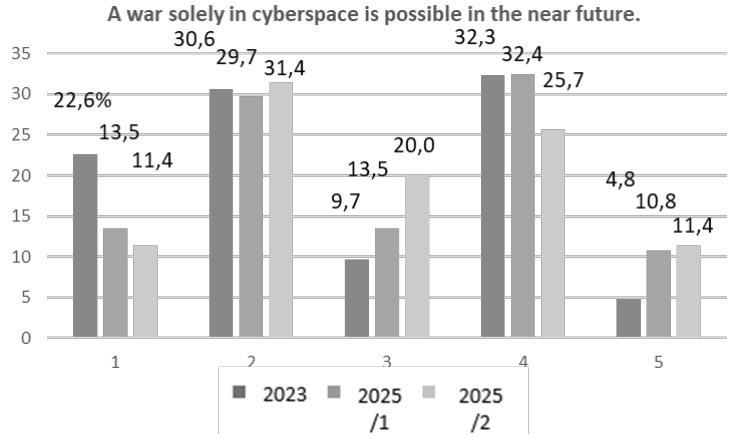

Figure 6: Answers to the question 6

5. Conclusions

Based on the overall analysis of the responses, three key observations can be made: 1) Key arguments for the acceptability of utilizing AI and cyber capabilities were that Finland need to keep up with technological developments and that also adversaries (Russia) actually use them; 2) The responses emphasized the requirement to include humans (Human-on-the-Loop) in decision-making; and 3) The officers also emphasized the comprehensibility and transparency of the production process of solutions made by AI or the information it produces to support decision-making.

As for the first observation, the concern is not unfounded and poses a strategic-normative dilemma for Western states committed to the international treaty regime (Dagen, 2025, 152). These last two requirements for AI are challenging because of the practical steps required to ensure that the military benefits sought by these systems are not compromised.

The requirement to keep humans involved in decision-making is justified on ethical grounds as well as for leadership and accountability. Soldiers have the right to use lethal force in certain situations, in which case the decision to use it and the responsibility for the consequences should lie with a human. On the other hand, the military commander will, in any case, make the decision, for example, to use an AI-enhanced or even AI-operated weapon system or to utilise AI for a specific task, in which case the decision-making will remain with a human. More important than keeping humans involved in military operations is the issue of leadership (Goldfarb & Lindsay, 2020, 5-8). AI cannot replace the example of a soldier’s ethos set by a military leader, strengthening the motivation of fighters, or understanding of human factors.

Understanding the production process of solutions or recommendations made by artificial intelligence is a more challenging issue. The software of an AI system is able to learn from its own experiences in addition to its training material. They can self-correct their algorithms and add or remove parameters, even if those changes no longer comply with the given rules. This can lead to a so-called "black box" phenomenon, where even the system designer or end user is unable to identify the changes or processes the system implements that result in certain solutions. (Chavannes & Arkhipov-Goyal, 2021, 71).

Although this study is not directly comparable with the U.S. and Australian studies due to, among other things, differences in the question wording and target groups (e.g., in terms of military education and cultural factors), some observations can be made. All studies emphasised that humans want to be involved in decision-making

and that trust in the use of AI to support military operations, e.g., in autonomous weapon systems, increases as officers understand its operating processes (Galliott & Wyatt, 2022, 270-271; Lushenko, 2023). Both Finnish and U.S. officers also considered that one of the key reasons for the use and development of military AI and autonomous weapon systems is that adversaries also develop and use them (Lushenko, 2023). The study confirmed perceptions of commitment to the military profession and decision-making based on expertise and knowledge.

Surveys conducted on military thought concretised the idea of a common understanding of prevailing threats, related to the constructive character of the war theory framework, against which material power must be developed using available technology, also in the cyber domain.

Military necessity strongly guided the attitude of Finnish officers towards the development and use of new technology and cyber capabilities for military purposes. Although a commitment to ethical aspects emerged, it is obvious that a small nation cannot afford moral superiority and thereby give significant advantages to the adversary.

Like U.S. general of the Army, Douglas MacArthur (1951) said: *"In war, there is no substitute for victory."*

References

Alkula, T., Pöntinen, S. and Ylöstalo, P. (1995) *Sosiaalitutkimuksen kvantitatiiviset menetelmät*. WSOY, Helsinki.

Boone, H. Jr. and Boone, D. (2012) Analyzing Likert Data, *Journal of Extension*, Volume 50, Number 2, Article Number 2TOT2, pp. 147–158.

Cannon, S. (2024) The Alliance's Transition to Multi-Domain Operations, Journal of Joint Air Power Competence Centre (37). https://www.japcc.org/articles/the-alliances-transition-to-multi-domainoperations/.

Cepik, M., Canabarro, D. and Ferreira, T. (2015) Cyberwar: Clausewitzian Encounters, *Space and Defense*, Vol. 8: No. 0, Article 5. DOI: 10.32873/uno.dc.sd.08.01.1125.

Chavannes, E. and Arkhipov-Goyal, A. (2021) The Ethics of Robotic and Autonomous Systems in a Military Context. https://www.jstor.org/stable/resrep29554.5.

Clarke, R. and Knake, R. (2010) *Cyber War: The Next Threat to National Security and What to do About it*. HarperCollins Publishers, New York 2010.

Clason, D. and Dormody, T. (1994) Analysing Data Measured by Individual Likert-type Items, *Journal of Agricultural Education*. Volume 35, Number 4, pp. 31–35.

Dagen, T. (2025) International Legal Challenges in Regulating the Use of Artificial Intelligence for Military and Peacekeeping Purposes. Review of European and Comparative Law, 2025. Vol. 63. No 4, 127-159.

Galliott, J. and Wyatt, A. (2022) A consideration of how emerging military leaders perceive themes in the autonomous weapon system discourse, Defence Studies, 22:2, 253-276.

Goldfarb, A. and Lindsay, J. (2020) Artificial intelligence in war: Human judgment as an organizational strength and a strategic liability. Brookings Institution.

Heikkilä, T. (2004) *Tilastollinen tutkimus*. Edita, Helsinki.

Hirsjärvi, S., Remes, P. and Sajavaara, P. (2015) *Tutki ja kirjoita.* Bookwell Oy, Porvoo.

Johnson, J. (2021) Artificial Intelligence and the Future of Warfare. The USA, China, and strategic stability. Manchester University Press.

Lehto, M. and Limnéll, J. (2017) Kybersodankäynnin kehityksestä ja tulevaisuudesta, *Tiede ja ase*, Vol 75. https://journal.fi/ta/article/view/67730.

Mazarr, M., Rhoades, A., Beauchamp-Mustafaga, N. et al (2022) *Disrupting Deterrence: Examining the Effects of Technologies on Strategic Deterrence in the 21st Century*. RAND Corporation, Santa Monica 2022.

MacArthur, D. (1951) Farewell Address to Congress. Delivered 19 April 1951, Washington, D.C.

Puusa, A., Juuti, P. and Aaltio, I. (2020) *Laadullisen Tutkimuksen Näkökulmat Ja Menetelmät*. Gaudeamus, Helsinki 2020.

Lushenko, P. (2023) AI & the future of warfare. Bulletin of the Atomic Scientists. https://thebulletin.org/2023/11/ai-and-the-future-of-warfare-the-troubling-evidence-from-the-us-military/.

Lushenko, P. (2024) Trust but verify: US Troops, artificial intelligence, and an uneasy partnership. https://mwi.westpoint.edu/trust-but-verify-us-troops-artificial-intelligence-and-an-uneasy-partnership/.

Raitasalo, J. and Sipilä, J. (2008) "Näkökulmia sotaan" Sota – teoria ja todellisuus. Näkökulmia sodan muutokseen. pp. 1-10. http://urn.fi/URN:ISBN:978-951-25-1894-4.

Saunders, M., Lewis, P. and Thornhill, A. (2012) *Research Methods for Business Students*. 6th edition, Pearson Education Limited, Essex.

Tähtinen, J. (2022) Sotilaallinen paha päivä: Venäjän 2000-luvun sotatoimien vaikutukset suomalaiseen sodan ja taistelun kuvaan sekä Suomen sotilaalliseen puolustukseen. https://urn.fi/URN:ISBN:978-951-25-3488-3.

Vego, M. (2011) On Military Theory. Issue 62, 3 d quarter 2011 / JFQ. https://apps.dtic.mil/sti/tr/pdf/ADA546600.pdf.

Vilander, J., Pulkka, A.-T., Erkkilä, V. and et al. (2019) Suomalaisten käsityksiä sodan sekä kyber- ja informaatiosodankäynnin uhkasta. Tiede Ja Ase, 2019(1). https://journal.fi/ta/article/view/88684.