DAIO Defense AI Observatory

Cautious Data-Driven Evolution

Defence AI in Finland

Sami O. Järvinen

DAIO Study 23|16

Ein Projekt im Rahmen von

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

About the Defense AI Observatory

The Defense AI Observatory (DAIO) at the Helmut Schmidt University in Hamburg monitors and analyzes the use of artificial intelligence by armed forces. DAIO comprises three interrelated work streams:

- Culture, concept development, and organizational transformation in the context of military innovation
- Current and future conflict pictures, conflict dynamics, and operational experience, especially related to the use of emerging technologies
- Defense industrial dynamics with a particular focus on the impact of emerging technologies on the nature and character of techno-industrial ecosystems

DAIO is an integral element of GhostPlay, a capability and technology development project for concept-driven and AI-enhanced defense decision-making in support of fast-paced defense operations. GhostPlay is funded by the Center for Digital and Technology Research of the German Bundeswehr (dtec.bw). dtec.bw is funded by the European Union – NextGenerationEU.

Ein Projekt im Rahmen von

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

Cautious Data-Driven Evolution

Defence AI in Finland

Sami O. Järvinen

DAIO Study 23|16

Ein Projekt im Rahmen von

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

About the Author

Sami O. Järvinen is Special Advisor at Defence Command Finland since 2016, specializing in Research and Development. His position involves coordination and implementation of the Finnish Defence Forces' R&D Strategy as well as various international projects, in particular with the European Defence Fund. Prior to joining the FDF, Järvinen worked as Senior Researcher for the Embassy of the Republic of Korea in Finland (2011–2016), as Programme Officer for the European Commission (2009–2010) and in several positions related to international cooperation at the Ministry for Foreign Affairs and the Ministry of the Environment of Finland (2005–2009). He holds a Master's degree in Sociology from the University of Jyväskylä.

Acknowledgments

The author would like to thank Prof. Pekka Appelqvist, Col Jyri Kosola, Col Jarkko Karsikas, LtCol Tero Solante, LtCol Petteri Hemminki, Dr. Terhi Rasilo, Dr. Heiko Borchert, Torben Schütz, and Joseph Verbovzsky for valuable comments and suggestions. The author is solely responsible for any errors in fact, analysis, or omission.

Design

Almasy Information Design Thinking

Imprint

Sami O. Järvinen, Cautious Data-Driven Evolution. Defence AI in Finland. DAIO Study 23/16 (Hamburg: Defense AI Observatory, 2023).

Defense AI Observatory | Chair of Political Theory | Helmut Schmidt University
Holstenhofweg 85 | 22043 Hamburg | T +49 40 6541 2776
www.defenseai.eu | contact@defenseai.eu | @Defense_AIO

ISSN (online): 2749–5337
ISSN (print): 2749–5345

Content

1 Summary

Finland has recognized AI as a top priority for technological and economic development, setting ambitious policy goals in the civilian sector. A national AI strategy was published in 2017 among the first countries in the world. In the defence sector, policy objectives are somewhat less ambitious, with a focus on general guidelines, piloting AI applications in administrative and support functions and only gradually proceeding to military capabilities.

Defence AI is most often tackled in the broader context of digitalization. The Finnish Defence Forces (FDF) implements a cross-cutting Digitalization Programme, identifying AI applications within FDF's internal development programs. Education of staff in order to better identify AI use cases and foster expertise for development and acquisition of AI systems is one key elements of the programme. National Defence University (NDU) incorporates AI in its curriculum at all levels.

Ethical and legal issues are being elaborated in a comprehensive way by Finnish defence experts. In particular, conceptual frameworks vis-à-vis Lethal Autonomous Weapon Systems (LAWS) have been developed seeking a pragmatic approach. In addition to delineating the general level of appropriate human involvement in the development and use of LAWS, the potential of AI for enhancing International Humanitarian Law (IHL) compliance is recognized.

The crucial importance of data is acknowledged by FDF for adequately exploiting the possibilities of AI, in particular machine learning. The availability of training data for developing AI applications needs to be ensured by tackling legal and organizational barriers, improving data storage systems, and enabling data sharing without compromising integrity and the appropriate protection of data.

The FDF R&D Strategy highlights AI as a priority research area. This is reflected in the R&D project portfolios of both the Ministry of Defence (MoD), the FDF and its NDU. Potential use cases for AI have been recognized in practically all areas of defence – the Ground Forces alone identified over 50 use cases in a recent study. Projects related to Robotics and Autonomous Systems are highlighted in this report as a particularly promising field of potential disruption. Dynamic management and exploitation of the electromagnetic spectrum is showcased as another area that might be revolutionized by AI in the near future.

At the national level, an ecosystem approach is applied to AI development both in the civilian and the defence sectors. Internally, the FDF applies a matrix organization in guiding and implementing AI applications.

International cooperation is used as a force multiplier for R&D, with EU and NATO being the main multilateral forums of cooperation and the U.S. and Sweden ranking among key bilateral partners. The ratification of Finland's NATO membership in April 2023 is opening a range of new possibilities for R&D cooperation.

Funding of AI development is in the order of hundreds of millions of euros nationally, in the civilian sectors, and tens of millions in the defence sector. Exact sums are impossible to estimate, but a fair share of the FDF annual €50M research budget involves AI, complemented by some portion of the more numerous and much bulkier other development programs of the FDF.

Fielding of AI applications seems to be taking baby steps. Defence systems currently in use in the Army, Navy and Air Forces only feature AI applications focusing on specific, narrow functions. Emphasis seems to be on AI-powered support functions, though it is to be suspected that publicly availably sources do not tell the whole story. Finland's acquisition of 64 F-35 fighters and the corresponding industrial cooperation with the U.S. will most likely propel FDF's use of AI to a new era within the next decade.

2 Thinking About Defense AI

In 2017, the Finnish Ministry of Economic Affairs created a task force with the objective of making Finland one of the frontrunners in global AI. Finland was among the first countries in the world to implement an AI policy program, *The Age of AI*, spanning 2017–2020. The work currently continues under the auspices of the follow-up program *Artificial Intelligence 4.0* launched in November 2020. The defence sector was quick to respond, with the Ministry of Defence providing strategic guidelines and the Defence Forces elaborating more concrete implementation programs and roadmaps.

2.1 Policy Guidelines

Published every four years, the *Government's Defence Report* is perhaps the most prestigious Finnish policy document on defence. In the latest *Defence Report* (2021), digitalization and artificial intelligence are recognized as prerequisites for developing national defence, as well as essential factors shaping the evolution of the operational environment.[1]

In the context of the development of military capabilities, the *Defence Report* highlights the role of digitalization and AI alongside with machine autonomy, sensor technologies and the emerging operational environments of cyber, space and the electromagnetic spectrum. Systems with various degrees of autonomy are being applied in ever intensifying and diversifying ways, accentuating the role of human-machine teaming. Even if the most dramatic effect of these technology trends may be seen in the domains of cyber, space and informational defence, the *Defence Report* recognizes that AI and digitalization will have an impact on *all* domains of defence. New technologies will find military applications, e.g., in information processing, situational awareness, management of weapon systems and logistics.[2]

The *Defence Report* notes that the performance of Finland's defence system is increasingly dependent on making use of digitalization and information management. The report outlines a broad objective for digitalization:

> to manage risks associated with emerging technologies, take advantage of opportunities, optimize activities, create new services, activities and knowledge, develop new abilities, and to be involved in national decisions. A key objective is to develop abilities related to utilising information and knowledge, and leading with knowledge, which can be reinforced with different artificial

1 Government's Defence Report, pp. 9, 16 and in particular p. 47.
2 Ibid., p. 16.

> intelligence applications. Applications can be used to improve the basis for decision making, since information will be available faster and it will be more accurate.[3]

Here, AI is mentioned in the context of information management, in particular vis-à-vis supporting and enhancing decision making.

The Ministry of Defence (MoD) published *Strategic Guidelines for Developing AI Solutions* in 2020, outlining a policy framework on the development and use of AI in the context of defence. Spanning from administrative requirements and building know-how to the foundations of implementation, the document sets five strategic guidelines. The objectives[4] are that

- defence policies and programs on AI be coherent, compatible and updated regularly;
- the research, development and maintenance of AI solutions be acquired in an agile manner;
- AI know-how be continuously improved via staff training and recruiting new experts;
- data be made available and used with flexible techniques based on up-to-date infrastructure; and
- the defence administration ensure the legality and solid ethical foundation of all of its AI applications.

2.2 Definitions of AI

A study commissioned by the Prime Minister's Office was published in 2018 with the aim of establishing a conceptual framework for AI in order to facilitate meaningful discussion and informed decision-making. The document identified AI as a crucial technological driver, enabling not just productivity increases but completely new ways of working, new processes and new business opportunities in multiple sectors. The study defined AI as software or technology that

> enables machines, programs, systems and services to function in a reasonable way as required by a given situation. A reasonable level of functioning necessitates the AI to be able to recognize different situations and environments and operate in accordance with how the situation evolves.[5]

3 Ibid., p. 48.
4 Ministry of Defence, *Strategic Guidelines for Developing AI Solutions*, p. 7.
5 Ailisto, *Tekoälyn käsitekartta*, p. 4.

The conceptual framework, based on the aforementioned study, cites another definition of AI referencing Russell and Norvig.[6] In their view, artificial intelligence is "*the designing and building of intelligent agents that receive percepts from the environment and take actions that affect that environment.*"[7]

The 2018 study and the conceptual framework*8* were influential in building foundations for the Government's thinking about AI. First and foremost, AI was firmly situated within the larger context of digitalization, and this conceptualization has proved to be durable across various defence policy documents.

Moreover, AI was recognized to be not a single technology, but a diverse group of methods, applications, technologies, and research areas cross-cutting multiple disciplines. The framework proposed a breakdown of the different expertise areas required for developing and applying AI into ten dimensions:[9]

1. Data analytics
2. Perception and situational awareness
3. Natural language and cognition
4. Human-machine interaction
5. Digital know-how in working life, problem-solving and computational creativity
6. Machine learning
7. System level and system effects
8. Computational environments, platforms, services and ecosystems for AI
9. Robotics and machine automation: the physical dimension of AI
10. Ethics, morality, regulation and legislation

This same conceptualization was later adopted in various other Government documents and has proven useful in making the discussion on military AI more lucid and concrete. The ten-dimensional framework was also featured in the Food for Thought paper "Digitalization and Artificial Intelligence in Defence," which Finland prepared in collaboration with Estonia, France, Germany and the Netherlands during Finland's EU Presidency of 2019.[10]

In the Finnish defence sector, no single consolidated definition of defence AI exists that would inform all the publicly available guiding documents. Many documents feature a very general, non-restrictive definition that carries little meaning in itself. Other documents recognize the diversity of existing definitions and propose

6 Russell/Norvig, *Artificial Intelligence: A Modern Approach.*
7 The wording adopted by the Finnish version of the document is somewhat different, stating that "AI enables machines, equipment, programs, systems and services to function in an intelligent or reasonable manner as required by the situation."
8 Ailisto, *Tekoälyn käsitekartta*, p. 4.
9 Ailisto, *Tekoälyn kokonaiskuva ja osaamiskartoitus*, p. 6.
10 Finland, Estonia, France, Germany, and the Netherlands, *Digitalization and Artificial Intelligence in Defence,* pp. 1–2.

some formulation of a working definition for the purposes of the scope of the document in question, without purporting to establish a definitive version.

The well-known distinction between Artificial Narrow Intelligence (ANI) or weak AI, and Artificial General Intelligence (AGI), or strong AI, does not feature prominently in the guiding documents of the defence sector. The *Strategic Guidelines* and its background study refer to current applications as ANI and even propose that we call them Assisting Intelligence instead of Artificial Intelligence.[11] AGI is seen as something futuristic, and while the diverse estimates of when it might be achieved are sometimes discussed, the documents do not comprehensively address the cartography leading from ANI to AGI. The 2018 Government study noted that all of the AI existing at the time was narrow AI.[12] Publicly available documents do not indicate that the defence administration foresaw the recent maturing and broad range of application of Large Language Models such as GPT-4.

The Finnish Defence Forces prepared an *AI Roadmap* in 2018,[13] which discusses several definitions of AI while also making use of the conceptual framework featuring in the 2018 study by the Prime Minister's Office. A working definition should include, at least, the components of data, calculation and modeling methods, computational environment, simulation and machine learning. BGen Mikko Heiskanen, then Chief of Defence Command C5, referred to the *Roadmap* highlighting that "*AI improves the predictability of operations and the accuracy and speed of decision-making by enabling a new kind of data analysis.*"[14]

The Ministry of Defence's *Strategic Guidelines for Developing AI* Solutions (2020) takes as a starting point the following very general definition: "*AI enables machines to perform tasks for which human intelligence has previously been required.*" The document goes on to specify that AI is best used for tasks where human intelligence falls short, for instance when the amount of data or required processing speed is too high, or if there is a "need for analysis independent of human factors."[15]

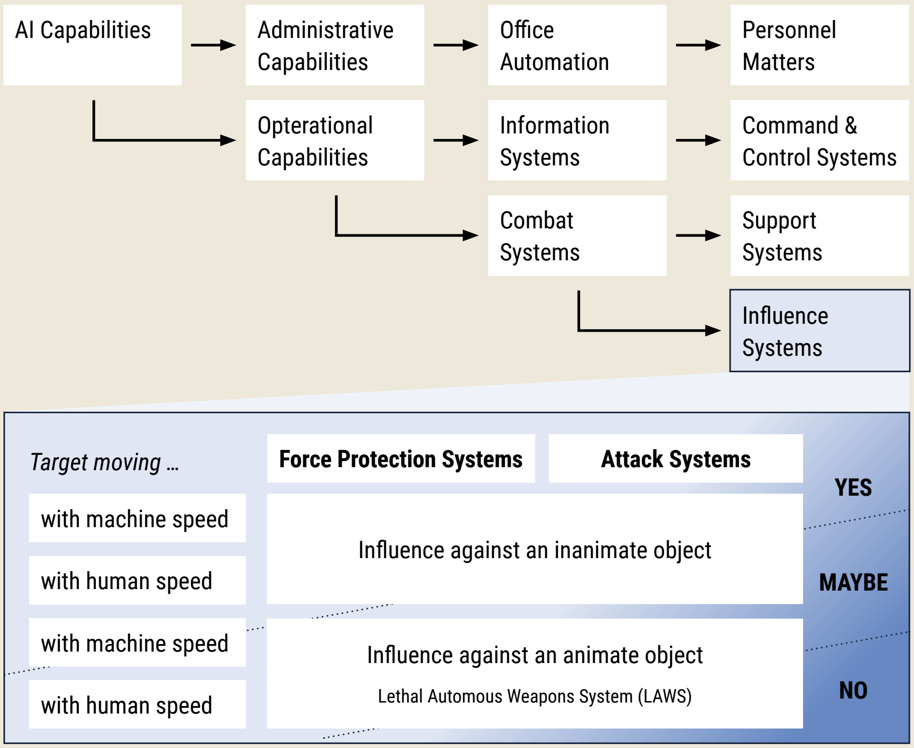
More importantly, the *Strategic Guidelines* also provide a classification of the areas of application of defence AI. The classification enables, among other things, to assess whether ethical and legal prerequisites are being met in a given project. As illustrated in Figure 1, *most applications of defence AI are unproblematic from a legal and ethical viewpoint* (that is, they are subject to the same stringent ethical

11 In Finnish this constitutes a pun, replacing *tekoäly* with *tukiäly*.
12 Ailisto, *Tekoälyn kokonaiskuva ja osaamiskartoitus*, p. 9.
13 The Roadmap is a classified document, but some elements of it have been publicly discussed. This article draws on those public presentations.
14 Heiskanen, *Puolustusvoimien näkökulmia tekoälyyn*, pp. 1–5.
15 *Strategic Guidelines for Developing AI Solutions*, p. 1.

and legal considerations as are non-AI applications). It is only when approaching the bottom right corner that AI-specific legal or ethical scruples may arise.

Some preliminary conclusions regarding the definition of military AI in Finland can now be proposed. Firstly, AI policy is mainly set in the broader context of digitalization. Secondly, AI is recognized to be an overarching notion with fuzzy boundaries, and it is often helpful to define it on a case-by-case basis, e.g., along the ten dimensions proposed by the 2018 conceptual framework. And thirdly, there is no "military AI" per se; rather, many different applications of AI are possible in a military context, and the overwhelming majority of them – but not all – are unproblematic from a legal and ethical standpoint. Nevertheless, a gray area does exist regarding Lethal Autonomous Weapon Systems (LAWS), which will be explored in chapter 2.3.

Figure 1: Categorization of AI Application Areas in Defence



Source: Strategic Guidelines for Developing AI Solutions, p. 3.

2.3 Ethics and Regulation of AI: Finland's Take on LAWS

The Government's Defence Report 2021 states that while "taking advantage of the opportunities provided by new technology, it is necessary to take into account the related *ethical challenges and legal limitations.*"[16] The MoD stresses the importance of complying with international legal and ethical obligations "in the construction and use of artificial intelligence," highlighting the role of legality and ethics as one of the five Strategic Guidelines for developing AI.[17]

Finland is fully committed to International Humanitarian Law (IHL) and an active proponent of its application to all aspects of warfare, including defence AI. Finnish defence experts point out that the same rules of IHL must in principle apply to autonomous weapon systems as to conventional forms of warfare. Special care must be taken in order to ensure that new weapon systems and military AI really comply with IHL in all circumstances.[18] However, the Finnish defence administration "does not self-regulate more stringently than what is required by law." The MoD stresses that national or international regulation must not prevent the development of ethically justified, necessary and appropriate AI based solutions.[19]

The MoD recognizes that a specific challenge is posed by hostile actors that do not comply with international regulation. National Defence University AI and autonomy researchers note that their work builds know-how in order to "prepare against a threat that does not adhere to international, commonly agreed restrictions on the use of autonomous weapons in the future battlefield."[20]

While cautious of the potential threats, the Finnish defence administration also recognizes the potential benefits of military AI and autonomous systems for improving IHL compliance of warfare. "*Artificial intelligence can also be used to reduce human suffering*," the Ministry of Defence notes in its guidelines on AI.[21] "*If AI enabled machine autonomy is applied to weapon systems with appropriate human involvement and by using ambitious ethical standards, it can also support humanitarian objectives, by allowing higher precision and distinction for military purposes.*"[22] An AI-enabled unmanned asset can get closer to its target than a manned unit would, therefore enabling far more precise situational awareness and targeting data. This may reduce collateral damage to civilians. Moreover, the

16 Government's Defence Report 2021, p. 48.
17 Strategic Guidelines for Developing AI Solutions, p. 7.
18 Finland, "Considerations on the appropriate level of human involvement in LAWS," pp. 1–3.
19 Strategic Guidelines for Developing AI Solutions, p. 3–4.
20 Nieminen et al., "Autonomia taistelukentällä – tulevaisuusorientoitunut tutkimus," p. 119.
21 Guidelines for Developing AI Solutions, p. 4.
22 Finland, "Elements for possible consensus recommendations," p. 3.

unmanned weapon can also abort its mission, if on-board AI infers that civilian collateral damage is imminent.

The defence administration participates in public discussion on the threats and opportunities of AI. On the intergovernmental level, Finland takes part in the processes under the United Nations Convention on Certain Conventional Weapons, notably via its Group of Governmental Experts (CCW GGE) on Lethal Autonomous Weapon Systems (LAWS).

A fixed and final national position on LAWS does not yet exist. Preconditions and potential elements for a national position can be found in expert-level Food for Thought papers contributed by Finland to the GGE and the EU.[23] These provide a starting point for establishing a conceptual framework delineating potential principles for the regulation of defence AI.

Grosso modo, it can be said that Finland does not advocate an outright ban on all weapon systems possessing a degree of autonomy, nor is it in favour of a *laissez-faire* policy of complete non-regulation. So far, no consensus has been reached even on the definition of LAWS. Regulation can still be advanced based on a jointly agreed categorization, classification, or characterization of AI.

Proposing a pragmatic way forward, Finland contributed a Food for Thought paper to the GGE in 2020 sketching a *framework for the appropriate level of human involvement* in LAWS. The five-phase framework seeks to outline the required level of human involvement to ensure IHL compliance in operational use: To ensure IHL compliant use of LAWS, the first phase is a rigorous and comprehensive *weapons review* in line with Article 36 of the 1st Additional Protocol to the Geneva Conventions. A second phase constitutes reviewing *military doctrines* and their operational and tactical implementation. The third phase review concerns *mission planning*, and, in particular, setting pre-defined boundaries for the operation of LAWS. The fourth phase deals with launch – to be decided by a human – and operation beyond the point-of-no-return, where human control is no longer present, but where advanced AI could still enable LAWS to analyze information and adapting its conduct. For instance, observing it has surpassed the boundaries preset for its operation, LAWS could adapt or abort the mission. The fifth and final phase of review concerns monitoring and ending of the mission.

A contribution to GGE in 2021 by Finland further elaborates a practical approach by identifying clear *boundaries for the application* of IHL vis-à-vis LAWS. The idea is that by stating the obvious, one can better delineate the non-obvious. Obvious

23 Finland, Estonia, France, Germany, and the Netherlands, "Digitalization and Artificial Intelligence in Defence;" Finland, "Considerations on the appropriate level of human involvement in LAWS;" Finland, "Elements for possible consensus recommendations."

cases violating IHL would include, e.g., a system (currently existing only in science fiction) that would be completely autonomous, operating beyond any human involvement. Conversely, many applications of military AI are clearly as unproblematic as traditional non-AI systems, for instance most dual-use technologies, solutions making use of AI as supporting elements of a weapon system controlled by humans etc.[24] The grey area, then, situated between the obvious cases, is where contextual assessment is always needed. In the grey area, no universal rules apply, but a case-by-case scrutiny will be necessary.

Work on the conceptual framework on ethics and regulation of lethal autonomous systems is still ongoing within the FDF. One particular area that will require extensive attention in the future is the implications of human-machine teaming for soldiers' social and ethical performance.[25]

2.4 Strategies and Programs of the Finnish Defence Forces

The Defence Forces' *AI Roadmap* of 2018 was a first attempt at an internal guiding document for applying AI in defence. It is intended to inform FDF decision-making but does not in itself constitute a decision. The document set an objective to create knowhow and capabilities for defining an operational and technical end-state during the 2020s. Long-term objectives for developing concrete applications were not defined: at that point, uncertainties were deemed so significant that it would be prudent to focus on identifying concrete applications in narrowly specified areas.

Thus, an *agile approach* was proposed: technical design should not be too refined or robust at too early a stage since that could lead to unwanted path-dependency. The *Roadmap* establishes an iterative, evolutionary approach instead of a revolutionary one, with a *modus operandi* of learning and verifying by doing. Existing AI technologies and products were to be applied more extensively, without, however, committing long-term to certain suppliers, technologies or products. The path would be reiterated step by step, and strategy formulated along the way. A framework was defined for the evolution of knowhow and organization for exploiting AI and controlling the threats it poses. Moreover, the *Roadmap* recognized the need for improving principles of data processing, and kickstarted processes to develop of machine learning and other AI functions supporting future defence capabilities.

24 Strategic Guidelines for Developing AI Solutions, p. 3
25 Aalto, "Autonomiset aseet ja etiikka," p. 46–48.

The *Roadmap* identified a series of use cases to be implemented in operative activities as well as supporting functions. While these cases have not been publicly discussed, BGen Heiskanen highlights the following special areas of interest in a presentation:[26] situational awareness and support for decision making; improved foresight; accelerating operational tempo; real-time sensor data fusion and analysis in service of situational awareness; stablishing and communicating situational awareness for cross-sectoral cooperation between authorities; and applying AI for training and real-time simulation.

The FDF Research and Development Strategy[27] (2019) highlights the role of AI as one of the priority areas for future R&D. Indeed, within the broad area of emerging technologies, artificial intelligence, cognition, and autonomy are a top priority. Potential AI applications will need to be assessed across a wide spectrum of areas, ranging from logistics to ISTAR, from decision-making and C2 to management of big data. Consequently, also the NDU's Department of Military Technology ranks *autonomy, robotics, AI and machine learning* as one of their five main research areas for 2022–2026.[28]

Critical technologies identified by the FDF include several areas that are influenced by or directly dependent on applying AI. These include, e.g., human and machine cognition, man-machine teaming, remote and autonomous systems, cognitive spectrum management, C2 and ISTAR, as well as positioning, navigation, and timing.[29] Moreover, sensor and data fusion is a crucial area of application for AI. The basis for leadership and situational awareness is a networked data system, which combines information produced via sensor fusion with an AI that analyzes it and provides solution proposals. FDF researchers point out that "[t]he impact of modern ground troops is based on data analyzed by AI from a wide selection of sensor sources."[30]

The FDF Digitalization Programme (2021, 2022) is the overarching internal document for setting the pace and principles for AI development and deployment across the defence system. Digitalization is defined as a cross-cutting functionality to be implemented via all of the FDF sectoral development programs. The document encompasses plans for educating and training personnel on AI, creating and nourishing a digitalization ecosystem, focusing on data, piloting a prototyping workshop activity, and establishing a process for gathering ideas as well as manag-

26 Heiskanen, Puolustusvoimien näkökulmia tekoälyyn, *pp. 1–4*.
27 The strategy is referenced here via the author's own unpublished presentations which have been cleared for publication by FDF.
28 Nieminen et al, "Autonomia taistelukentällä – tulevaisuusorientoitunut tutkimus," p. 119.
29 Kosola's presentation 22 November 2022 at ASDA seminar, unpublished.
30 Tiilikka et al., "Taistelija-hanke," p 124.

ing risks. Moreover, development processes need to be rendered more agile while promoting an organizational culture that encourages sharing and innovation.[31]

The *Digitalization Programme* identifies processes and measures for harnessing digitalization as an engine of change and enhances the understanding of FDF staff on the possibilities of digitalization for developing military capabilities. Concrete development projects will be based on selected use cases, with process owners in each service or branch leading their respective projects. As one of the guiding principles, the Digitalization Programme highlights the central role of *data* as a prerequisite for making use of AI.

2.5 Key Enabler: Data

Data is pivotal for digitalization and AI. The MoD notes that "the amount of data has increased exponentially, which means that more efficient methods are needed to deal with it."[32] The importance of the availability of data was recognized in Finland's EU Presidency *Food for Thought* paper (2019), which noted that there are obstacles for exchanging data even within the armed forces of one country, not to mention for the international sharing of data. Data needs to be stored and classified in such a way that will enable flexible and appropriate use in applications and pave the way for increased cooperation between EU and NATO member states. Indeed, one of the strengths of the EU is the striving for joint procurement of materiel, pooling and sharing of equipment – and exchange of experiences and data.

The *FDF Digitalization Programme*[33] highlights the central role of data for improving current capabilities as well as enabling new capabilities. This requires, on the one hand, that relevant data be made available e.g., for training AI applications, and on the other hand, that infrastructure and computational models be capable of handling the increasingly voluminous data masses. The quality and quantity of data play a crucial role for making use of machine learning in complex processes: data is what the AI algorithms are trained on. The fact that certain databases central for developing machine learning solutions are owned by giant international corporations may make it difficult for Finnish developers to excel in such subfields.

Various obstacles may hinder the efficient use of data, for instance if data is protected in such a way that relevant stakeholders cannot access it, or if data is stuck

31 Karsikas, "Puolustusvoimien digitalisaatio valmistaa huomisen haasteisiin."
32 Strategic Guidelines for Developing AI Solutions, p. 2.
33 Karsikas, "Puolustusvoimien digitalisaatio valmistaa huomisen haasteisiin."

in silos due to organizational barriers, incompatible formats or sloppy structuring. However, based on recent milestones in the development of civilian AI, it can be predicted that AI can even be trained on unstructured data in the very near future. A special hurdle is posed by Finnish data protection legislation, which prevents the authorities, among other things, from using data in a database for any other reason than the one it was collected for.

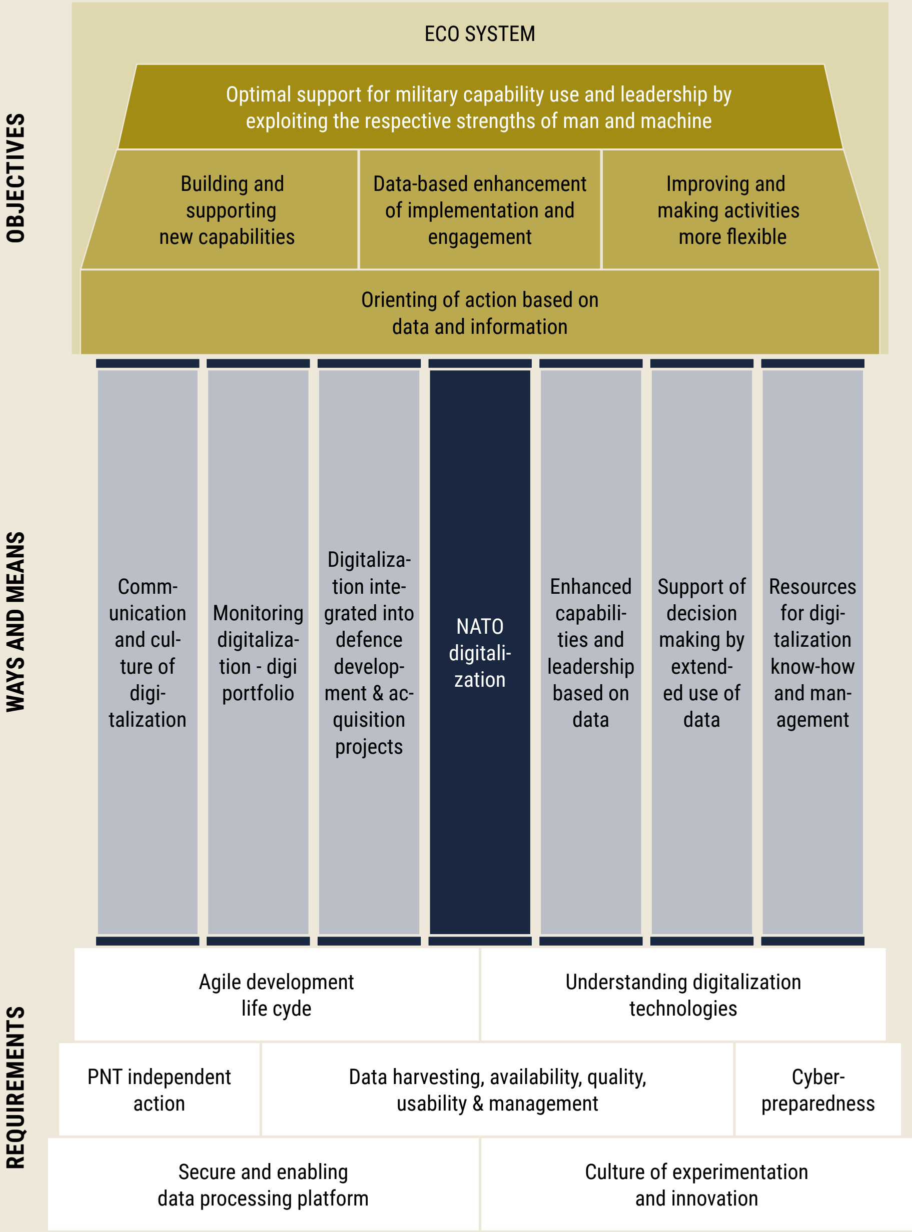
The need for modifying and improving the principles of data processing was observed already in the FDF's *AI Roadmap* of 2018.[34] NDU researchers Petteri Hemminki, Kai Virtanen, and Kimmo Halunen point out that the availability of teaching data is a key challenge for machine learning. They caution that supplier selection for data gathering, management and storage solutions may inadvertently grant the supplier an advantage that may be unfair or even unproductive. The procurer must be alert, protecting the data used for training AI, so that the procurer retains full authority for future development of the solutions, also ensuring integrity against cyber threats. Turnkey procurement of AI systems is a potential pitfall for the uneducated client.[35] As a workaround, the use of synthetic data is considered in certain projects.

The FDF is preparing a new Data Concept aimed at supporting the planning and use of the defence system by fostering better and more cross-cutting availability of data in order to enable multi-domain operations jointly with allies. The guiding principle is to use data to support military and political decision making, based on an improved situational awareness. Ideally, situational awareness data will be compiled jointly from all NATO members in all domains. This will enable effective joint operations, including enhanced joint fires with an "any sensor to any shooter" approach.[36]

Achieving the objective of the new Data Concept requires that data not be confined in silos but rather be made accessible between services and subsystems. In practice, this implies a paradigm shift in data security thinking – from "need to know" towards "need to share." The new paradigm would include Data-Centric Security (DCS), based on protecting data instead of protecting information systems. The objective is to combine data protection and data sharing in an unhindered manner. Security controls and mechanisms of protection and sharing are aimed at the data itself instead of at the information systems. DCS requires an advanced capacity for defining and classifying data, including automatic data labeling, binding with metadata and new crypto solutions. DCS is also an integral

34 Heiskanen, Puolustusvoimien näkökulmia tekoälyyn, pp. 1–3.
35 Hemmink/Virtanen/Halunen, "Tekoälyn kehityksellä autonomiaa asejärjestelmiin – mihin pitäisi varautua?," p. 235.
36 Interview with FDF CDO Tero Solante, Helsinki, 29 June 2023. The FDF Data Concept is a classified document and currently exists only as a draft, so its contents are addressed here only at the level of general guiding principles.

Figure 2: Principles of FDF Digitalization Architecture



Source: FDF (unpublished)

PNT: Position, Navigation, and Timing

part of the data architecture of NATO and its key partners; its implementation in FDF has received an additional impetus from Finland's NATO membership.[37]

The guiding principles of FDF's digital architecture can be illustrated as a house, with objectives serving as the "roof," implementation measures as the supports, and basic requirements as its foundation (see Figure 2). The foundation must be built first: a culture of experimentation and innovation, agile methodologies, availability of secure and high-quality data etc. Next come the supporting pillars, illustrated by different means of implementation. It is notable that the fourth pillar was added after Finland's NATO membership was ratified on 4 April 2023. The "roof" includes the most important objectives: to build and support military capabilities.[38]

2.6 Conclusions on Military AI Policy Guidelines

Across the various strategies and programs on military AI, certain recurring principles begin to emerge. AI is generally recognized to be a cross-cutting issue; consequently, a dedicated defence AI agency would not make sense. Rather, the defence sector seeks to identify and implement AI solutions in a capability-specific way.

Publicly available MoD and FDF documents give the impression that the low-hanging fruits for AI application are being sought through cost-savings and efficiency gains in administrative and support functions. Enhancing existing military capabilities is often mentioned as one item on a list, and the development of completely new capabilities based on AI is only hinted at. Doctrinal thinking is not publicly discussed, but possible elements for concepts and doctrines on AI application can be inferred from published documents.

For the division of roles between man and machine, the latter has often been relegated tasks that are deemed dull, dirty or dangerous (3D). Any process or event that recurs frequently is a natural candidate for automation. Should the mission require that the machine possess some degree of situational awareness or a capability to operate without constant human supervision, the system will necessarily involve elements of AI. Conversely, if the tasks are simple enough, autonomous capacities may not be required, if a simple mechanical or automated solution will do.[39]

37 Ibid.
38 Ibid.
39 Hemminki/Virtanen/Halunen,"Tekoälyn kehityksellä autonomiaa asejärjestelmiin – mihin pitäisi varautua?," p. 213.

Automation can also improve cost-effectiveness as well as reduce the cognitive burden of humans. This aspect has been identified as one of the low hanging fruits of AI by especially the early Finnish AI strategies. Rather than searching for completely new ways of warfighting or achieving superhuman performance in a given task, the first defence AI policy documents would stress the seemingly harmless objective of achieving the same things as before but at a reduced cost. Such a banal approach, however, is only seemingly harmless, since the price of missing out on disruptive battlefield innovations could prove to be high.

In addition to the 3D and cutting costs, AI can also bring a real force multiplier or even a disruption. In cases where the amount of data exceeds human processing capacity or where the situation requires superhuman reaction speeds, automated or AI systems can help. Moreover, systems with increasing autonomous capacities may prove to be the next revolution in military affairs, enabling completely new concepts of warfighting.

3 Developing Defense AI

This chapter introduces the principles and main structures of FDF development work. Next, some of the potential uses for AI are outlined. One broad field of application, remote autonomous systems, is highlighted as an example of potential disruption enabled by AI, and a selection of related R&D projects is introduced, followed by a few other R&D project cases. This selection of projects is not intended as exhaustive – it may not even be a representative sample, since the main selection criteria has been the availability of information. The highest technology readiness level (TRL) projects and all of acquisition are left out since data on their contents is not publicly available. Moreover, since FDF concepts and doctrines are also not public, the conceptual thinking presented below draws from Finnish public sources that may only provide some potential elements identified, but they are not to be taken as connected with actual doctrine or concepts.

3.1 FDF R&D: Rationale and Modus Operandi

The Finnish Defence Forces conduct research and development in order to generate knowledge that supports decision-making and to create the technological basis and knowhow for building and maintaining military capabilities. As Finland is a small country with a specialized but limited defence industry, much of the defence materiel is procured off the shelf.[40] Consequently, much of FDF R&D focuses on experimentation, testing and integration. However, certain capabilities may need to be developed nationally or through international cooperation, and to the extent that this is the case, the role of in-house R&D is accentuated. Low-TRL research can be funded via public calls, such as the annual MATINE funding that connects the defence sector with academia and research institutes. The most promising projects are taken up for targeted funding at a higher TRL, with the FDF Research Program being the spearhead R&D funding mechanism. International cooperation can also be used as a force multiplier via, *inter alia*, NATO, the European Defence Agency (EDA) and the European Defence Fund (EDF). Finally, after the industries have completed the highest TRL tiers, acquisition of defence materiel takes place through the FDF Development Programs.

MATINE or the Scientific Advisory Board for Defence is a special structure established to ensure an active link between the worlds of academic and civilian research and the defence community. It promotes defense and security research while also functioning as a network of over 300 scientists. MATINE gives university professors a window into defence matters, while functioning as a multidisciplinary

40 However, the recently published *Defence Materiel Policy Strategy* states that "it is essential for national security that Finnish companies have an adequate technological level of know-how of critical technologies. Especially in digitalization, AI, analytics and autonomy the security of supply for national know-how is an area of growing importance" (MoD, *Puolustushallinnon materiaalipoliittinen strategia 2023*, p. 8). This reflects the increasing need for sovereignty in critical defence technologies.

think tank for the Defence Forces by providing a direct channel into latest research and prospects. MATINE's research funding focuses on projects that are too risky or too low TRL to receive direct FDF funding, but that have disruptive potential for defence capability development. The most successful MATINE projects can be upscaled with FDF funding. Examples of recent MATINE-funded research projects featuring AI applications will be discussed below.

The Finnish Defence Forces' Research Program can be considered a kind of spearhead of FDF research work. The current program (2021–2025) features several projects exploiting the potential of AI. The Research Program benefits from a particular feature of the Finnish society, the long tradition of general conscription: since most men have completed military training, R&D procured from Finnish companies is inherently carried out by people with a hands-on military understanding.

While the detailed research objectives have not been published, the publicly available project titles give a hint as to how extensively AI permeates the current R&D work of FDF: the Situational Awareness portfolio of the program includes such projects as AI for Detection and Classification of Radar Signals; AI as Situational Awareness Operator and Analytical Support; Producing Situational Awareness with a Drone; AI in Processing Big Data Masses; and Target Situational Awareness and Sensor Fusion. Another portfolio is entitled Human-Machine Teaming, and it features projects like Autonomous Systems for Surveillance and Engagement; and Technology and AI-Powered Development of Operations.

International cooperation is a force multiplier for R&D. Finland is active in NATO's Science and Technology Organization, participating in more than 70 activities, many of which focus on AI. Much of FDF multilateral R&D cooperation is carried out within the European Defence Agency as well as the European Defence Fund and its predecessors. Military uses of robotics and AI have also been conceptually explored within the Multinational Capability Development Campaign (MCDC).

3.2 Potential Uses of AI

As demonstrated in Figure 1, there are multiple potential use cases for AI applications, but the majority of them pertain to other systems than kinetic weapons. The following is an attempt to summarize, based on publicly available sources, what types of use cases the FDF has identified as potential building blocks of AI-enabled capacities.[41]

41 The list may not be exhaustive, and it is particularly noteworthy that doctrine and concepts of operation as well as related planning documents are classified; therefore, this listing does not cover the actual extent of application.

AI could assist in forming troops by optimizing the assignment of tasks and missions, by providing a personal assistant to conscripts or monitoring the performance of soldiers or groups. Moreover, conscription could even be revolutionized by the introduction of virtual elements whereby a select portion of the training could be tailor-made and executed remotely. AI can support leadership and decision-making by compiling and analyzing situational awareness data,[42] by formulating proposals and assessing the potential implications of decisions, by drafting orders and instructions as well as by synchronizing and monitoring execution. Moreover, AI could be used to simulate alternative decisions across a number of scenarios far exceeding human processing capacity:

- **Intelligence:** Intelligence can be improved via AI applications. The constantly growing computational capacity of sensor systems along with predictive analysis enable a more and more complete and up-to-date situational awareness. Image recognition software is constantly improving and has in certain cases already surpassed human capability. Often the best performance can be achieved by applying AI in combination with human judgement, making use of the virtues of each.

- **Electromagnetic and Cyber Domain:** Ubiquitous digitalization opens up new pathways for intelligent data gathering from the electromagnetic spectrum as well as from the internet. As demonstrated by the war in Ukraine, even data from social media can quickly transform into target acquisition. The cyber domain is a well-established area for AI for both defensive and offensive applications. Information warfare may be heavily exacerbated by AI which enables the automatic monitoring and targeting of people with fairly low resources[43] – a threat scenario to prepare against.

- **Logistics:** Logistics is already being constantly optimized via such AI-powered processes as predictive maintenance, and the automatization of stock and transport management. Military medicine is improving via e.g., preventive precision medication enabled by AI, and new ways of constantly measuring human performance and optimizing its restoration are also made possible by AI systems. Searching for wounded soldiers can be improved by drones, and their evacuation can be carried out by UGVs with increasingly autonomous capabilities. Progress in most of these areas is driven by civilian technology, but the defence sector is actively searching for ways to apply them in the battlefield.

42 Kallinen, "Kognitiivinen sodankäynti," pp. 50–52.
43 Kosola, "Hyvä – paha digitalisaatio," p. 69.

- **Force Protection and Engagement:** More military-specific applications of AI include force protection and engagement. Protection can be enhanced by AI application via improved detection and identification of threats and automation of countermeasures on the one hand, and via improved techniques of concealment, decoys or misleading the enemy. Engagement can be enhanced if the planning of kinetic force is improved via AI techniques; collateral damage could be reduced with AI-powered risk assessments; and AI can also enable advanced cyber or electronic warfare functionalities. Notably, AI applications can be used to enhance joint fires by exploiting targeting data from any sensor to any shooter.[44]

- **Acceleration Decision-Making:** Another disruptive element that AI may bring to the battlefield is accelerating the observe, orient, decide, act (OODA) loop at each phase. Decentralized AI applications, either in the physical domain in the form of robot swarms or as software agents operating in networks, can help to achieve a superior tempo of operations.[45] Finally, an emerging game changer partly enabled by the development of AI is the application of unmanned systems with autonomous capabilities.

3.3 The Next Disruption: Remote Autonomous Systems

FDF Research Director Jyri Kosola estimates that the next disruption in warfare will be propelled mainly by unmanned systems and the combination of AI, digitalization and data.[46] Analyzing the possible ways in which robotic and autonomous systems could disrupt the battlefield,[47] Kosola notes that unmanned sensor and weapon platforms can either act as a force multiplier for existing concepts or enable completely new doctrines of fighting. For instance, a traditional minefield based on guessing where the enemy might move and then deploying masses of stationary mines might be rendered obsolete by smart mines.[48] Areas and pathways to be denied could be decided only hours before the event, and moving mines with targeting capacity free engineers from predicting enemy moves and

44 Interview with FDF CDO Tero Solante, Helsinki, 29 June 2023. He highlights that after Finland's admission to NATO in April 2023, the emphasis in data concept development is shifting from administrative and support functions towards kinetic engagement.
45 Kosola, "Naton teknologianäkymiä vuoteen 2040," p. 75.
46 Kosola, "Naton teknologianäkymiä vuoteen 2040," p. 78.
47 These publicly available texts do not represent an FDF position, and there is no publicly available FDF roadmap or concept related to unmanned/autonomous systems. Lacking any publicly released official doctrine or roadmap, we can examine Kosola's publicly expressed views as possible elements of what FDF research, development and planning should consider.
48 Kosola, "Paradigman muutos," p. 65.

making time-consuming installations. Moreover, fewer mines would suffice – and blue force can pass through.

As the development of AI and sensor technologies enables machines to become increasingly aware of their own state and their environment, they become increasingly autonomous, requiring less external control. This evolution is expected to result in combat teams consisting of humans and machines in the 2030s. An appropriate division of labor retains humans in control of decision-making and monitoring, based on human capacity for situational awareness and contextual judgment. Correspondingly, the machine would play the implementing role, especially for 3D missions as well as situations requiring superhuman execution speed.[49]

How to use this disruption to gain operational advantage? Kosola reasons that this requires defining the man-machine division of labor already at the very planning stage of operational concepts, thereby optimizing the machine for its mission and conditions. For instance, an unmanned platform can be much smaller, since it doesn't have to have space, life support or protection for a human. This enables improved mobility and resilience. The unmanned platform can also be more difficult to detect, enabling it to operate nearer its target.

A potential concept starts to emerge, one based on multiple small, inexpensive and expendable platforms operating in a swarm-like fashion. Each unit in itself may be much less capable than a large and expensive platform, but their large quantity more than compensates for the inferior quality. Expendability enables for completely new concepts of operation. Kosola refers to *mosaic warfare* as opposed to monolithic capabilities. The swarm, enabled by AI-powered autonomous features, is stronger and more resilient than a corresponding monolithic capability.[50]

While these reflections do not necessarily reflect existing or even emerging FDF doctrine, they provide some insight into possible pathways into future capabilities. Many FDF research projects aim at creating a knowledge base and developing technological enablers that could be used as elements for various systems involving remote and autonomous platforms. A few such projects are introduced below.

49 Kosola, "Sodankäyntiä muuttavat teknologiset ilmiöt," pp. 70–74.
50 Kosola, "Palapelin rakentelua vai peliä mosaiikilla," pp. 74–78.

Enablers for Autonomous Systems: Case iMUGS

Finland participates in the EU-funded R&D project Integrated Modular Unmanned Ground Systems (iMUGS). Led by the Estonian company Milrem, the project aims at enhancing the autonomous features of unmanned systems and facilitating joint operation of machines and humans. The FDF has a multiple interest in the project, the main objective being to develop knowhow, technologies and standards that could function as enablers in various unmanned systems of the future, irrespective of supplier. One aspect is evaluating the use of unmanned platforms as part of cooperative man-machine teams. The rationale is to deploy unmanned assets as part of a man-machine troop in order to mitigate threat and reduce casualties for civilians and blue combat forces, to improve situational awareness, to prevent misjudgment caused by tiredness or stress as well as to enhance military performance in situations that overwhelm human reaction speed.[51] The FDF's overarching goal is to develop know-how and enabler technologies that can be used across various different unmanned platforms and systems.

Such enablers include C2 systems and navigation solutions capable of operating in GNSS denied environments; sensors and algorithms enabling the platforms to cooperate. All of these also need to be resilient to cyber and electronic attacks as well as arctic conditions. Most elements of the iMUGS architecture are designed to be modular, open, and scalable. The iMUGS UGVs can be equipped with different payloads ranging from different sensors, bomb disarmament or mine clearing equipment and firefighting gear to weapons such as anti-tank missiles or a machine gun. In the EU-funded iMUGS project, all testing is done with an unarmed platform. Evacuation missions and ammunition resupply logistics have been successfully demonstrated over various scenarios.

The iMUGS project is currently in its concluding phase with final demonstrations showcasing a more advanced level of autonomy for the UGV platforms as before. The UGVs are capable of maneuvering autonomously to pre-planned battle positions, choosing their own trajectory as well as detecting obstacles and adapting their navigation accordingly, both in line of sight and beyond. These feats are, however, performed in a somewhat simplified environment. Autonomous navigation across a complex terrain such as thick forest still remains to be demonstrated in a way that would be consistent enough to allow for reliable operational use. Swarming capabilities have been developed for conditions where a link to a central controller is present ("global swarming") and where it is absent ("local swarming"). In the swarming demonstrations, emphasis is still in virtual simulations, but with the potential for real-world application and upscaling.

51 Harju, "Puolustusvoimat testasi maarobottia, josta voisi tulla suomalaissotilaiden taisteluapulainen 2030-luvulla."

AI applications feature in numerous work packages within the iMUGS project. Insta applies machine learning methods developing and optimizing the *local swarming* algorithms, including for mission level path planning as well as for optimizing swarm behavior in selected use cases. In the *global swarming* work package, implemented by dotOcean, AI application is limited to clustering algorithms for solving problems related to the planning of swarming. The iMUGS communications solution developed by Bittium has been designed to support various AI applications, e.g., for situational and spectral awareness and optimization of network performance. At the communication node level, the system is capable of running AI algorithms for analysis and classification of node data, while at network level, AI applications may be used for smart routing and dynamic spectrum management. Moreover, a concept of distributed AI has been studied to identify further possibilities. Finally, the Autonomy Kit responsible for the autonomous mobility of the UGV platform features several AI-based elements developed by Safran: a person and vehicle detection module and a path detection functionality based a deep learning solutions, and a waypoint navigation module based on an AI domain called constraints programming and solving.

The FDF is currently exploring possible use cases for systems featuring unmanned platforms with autonomous capabilities and reflecting them to the needs of the Finnish Ground Forces in the 2030s. UGVs with a relatively high level of autonomous capability might be operational on the battlefield perhaps in a decade. The iMUGS project is experimental, in the sense that FDF is not procuring a mature device but developing concepts for versatile human-machine interactions.[52] The main Finnish companies involved are Bittium, providing network communication data link systems, and Insta, developing swarming features. Both technology areas will be essential elements in any AI-based unmanned future system with autonomous capabilities.

Experimental Platform for Autonomy Research: Case Laykka-AMPGV

The NDU's faculty of military technology is collaborating with various other universities on future-oriented experimental research on potential combinations of narrow AI functions. One research area focuses on systems that have autonomous capabilities and their impact on the future battlefield. This can be explored by creating concept models in a virtual environment and testing them across different scenarios. The results of the simulations are subsequently verified by constructing and integrating several functionalities of narrow AI into a common multipurpose platform and by testing them in actual terrain conditions corresponding to the

52 Ibid.

simulated environment.[53] Many research projects currently revolve around the experimental micro UGV platform Laykka.

Developed for the Finnish Defence Forces in collaboration with the University of Tampere and the National Defence University, Laykka-AMPGV (Autonomous Multi-Purpose Ground Vehicle) is an experimental unmanned ground vehicle aimed at performing a variety of functions depending on its payload. Having passed tests at demonstrator level, Laykka is currently being developed towards prototype and eventually to fieldable product.[54]

Weighing only 100 kg, Laykka's primary use might be stealthy anti-tank missions, removing the human from the extremely dangerous task of destroying enemy battle tanks. Laykka could also perform a variety of other functions ranging from intelligence missions to automatized patrolling and logistics tasks or forming a "smart mine field." Other possible use cases include medical evacuation, transport of ammunition, mobile communications relay station, charging base for a UAV – or a loitering weapon.[55]

Laykka can revolutionize the notion of minefields: instead of mines being permanently placed at fixed locations, the mines can loiter for long times but also move around as necessary while the situation unfolds. In this puzzle, the UGV platform is only one piece, while other elements of the system would necessarily involve tools for maintaining situational awareness, swarming capabilities for coordinating with other units and so on.

Several research topics are linked to the Laykka platform aiming at the development of various elements of autonomy and AI applications. One such study is developing solutions for military medicine, in particular casualty evacuation. Another study focused on image recognition, developing visual identification and classification of military vehicles via neural net algorithms. While the system reached a 90% accuracy with a data set of only 6000 images, achieving a necessary 99% accuracy in all real battlefield conditions (including seasonal changes, terrain features and camouflage) would require years of additional study with millions of data points. The NDU is engaged in this data collection work via Laykka as well as the MULTICO project.[56]

53 Nieminen et al., "Autonomia taistelukentällä – tulevaisuusorientoitunut tutkimus," p. 119.
54 Andersson, "Laykka-AMPGV:n inkrementaalinen kehitysprosessi runkoversio X.2:sta X.3:een sekä kehityksen seuranta kenttätesteillä ja -kokeella," p. 1–4.
55 Hemminki/Virtanen/Halunen, "Tekoälyn kehityksellä autonomiaa asejärjestelmiin – mihin pitäisi varautua?," p. 229.
56 Ibid., p. 226.

Autonomous Sensing Using Satellites, Multicopters, Sensors and Actuators: MULTICO

The MULTICO project is a prime example of research cooperation between civil and military companies, academia and the FDF. With the objective of producing real-time situational awareness from data produced by minisatellites, multicopters and other sensor systems, the project is carried out by companies and research institutions with the FDF providing military expertise. The project aims at the civilian markets, but FDF involvement ensures that applications with military relevance will meet corresponding requirements to be deployable on the battlefield.

Elements being developed within the MULTICO system include GNSS independent navigation (Aalto University), operating drones as an autonomous swarm (Nokia, SAAB, Aalto), gathering sensor data from radars (SAAB Finland), miniature SAR imagery from drones (DA Group) and satellites (ICEYE), hyperspectral imaging, data fusion and system integration (VTT). AI applications pervade the entire project, powering data fusion and enabling the swarming capabilities of sensor carrying platforms. Many of the solutions developed will find immediate military solutions, while other cases may require further development meeting special requirements of robustness, resilience to interference, A2AD etc.

Cooperative Testing and Development of Manned-Unmanned Teaming: MUM-T

FDF participates in an Airbus-led project with the German Bundeswehr aiming to develop and demonstrate capabilities of manned-unmanned teaming (MUM-T). Part of the Future Combat Air System (FCAS), the MUM-T project achieved a major milestone in a Multi-Domain Flight Demo held in Rovajärvi, Finland in the summer of 2022: in Europe's first large-scale multi-domain flight demo, two fighter jets, one helicopter and five unmanned remote carriers teamed up executing a mission in a real-life inspired scenario and under near operational conditions.[57]

In the demonstration, the fighter jets, helicopter ,and unmanned drones were connected via a meshed networking data link provided by Patria, allowing them to seamlessly interact, negotiate division of labor and switch control of unmanned platforms between several manned units. The remote carriers were commanded by human crew aboard a fighter jet, but executed much of their given mission autonomously. Two drones with electromagnetic sensor payloads were tasked to detect enemy air defence positions while three drones provided visual confirmation with electro-optical cameras. With the target acquisition data from the drones,

57 For more information, see: https://www.airbus.com/en/products-services/defence/uas/uas-solutions/manned-unmanned-teaming-mut-t (last accessed 10 July 2023).

the fighter jet proceeded to eliminate the air defence. Moreover, a helicopter provided close air support, teaming up with one of the electro-optical drones for gathering additional reconnaissance data.

The next phase of the project is expected to lead to maturing of existing capabilities and development of new ones, such as developing novel drone platform prototype and as well as first MUM-T tests with an existing fighter aircraft within the next years.

Swarming Capabilities for Unmanned Systems

Various projects are underway in order to develop swarming capabilities of unmanned platforms for a wide range of purposes. Alongside with the algorithms that Insta is developing within the iMUGS project, another project co-funded by MATINE and led by Patria explores the potential of drone swarm intelligence for intelligence, surveillance and targeting.[58] In order to succeed using swarm intelligence in a military context, the developers need to have an in-depth understanding of the field (including platforms, sensor, targets, and threats). Therefore, the swarming algorithms can become fairly complex. The project merges sensor data from electro-optic, infra-red, and SAR sensors.

Results indicate that data volumes gathered and transmitted grow very large in scenarios where full autonomy is applied. Scenario testing on different combinations showed that EO, IR and SAR sensor payloads and timing of platforms can be optimized for either maximal coverage, maximal speed of identification of targets or minimal usage of data and energy. Swarming capacity will need to be further developed, e.g., by improved or alternative platforms, more elaborate modeling of flight mechanics, enhancing the performance modeling for detection, recognition and identification of targets via tactical use of sensors, trajectory optimization, and novel swarming algorithms.

58 For more information, see: https://www.defmin.fi/files/5549/1330_MATINE_2500M-0133_Tutkimusseminaari_2022_Patria_Jylha.pdf (last accessed 10 July 2023)

3.4 Dynamic Electromagnetic Spectrum Management

One area where AI may fuel a potential breakthrough is dynamic electromagnetic spectrum management (EMSM). Future communications, radar and electronic warfare systems may have cognitive capacities, allowing them to use the electromagnetic spectrum in a dynamic way: A software-based transceiver could use AI to analyze the available spectrum, making optimal use of the spatially and temporally available bands and generating new waveforms depending on the frequencies available. With machine learning, the system could also extrapolate from previous experiences while adapting to new situations (cognitive spectrum management). Ideally, the AI would learn to avoid interfering with civilian and blue force communications by dynamic use of frequency bands, and could even execute simultaneous jamming or spoofing of enemy signals while providing blue force C2. The latter capabilities could be based, e.g., on signal modulation or polarization, combined with dynamic adjustment of output power. Moreover, machine learning may enable electronic warfare and intelligence systems to autonomously provide situational awareness of the spectrum and to identify anomalous signals and equipment.

While dynamic EMSM is an emerging area for R&D, the main hurdle for fully exploiting such systems might not be technological but regulatory. Current regulation of the use of the electromagnetic spectrum is fairly inflexible: the legislation simply divides the spectrum into frequency bands, which are then granted for or prohibited from use by defined operators. The law does not provide for spatial or temporal flexibility.

4 Organizing Defense AI

On the national level, an ecosystem approach is applied both to the development of civilian AI and to the digitalization of defence. Within the FDF, no specialized AI agency has been established, but instead a matrix-type organization is in charge of promoting the cross-cutting development of AI.

4.1 Civilian AI Ecosystem

The Government's *Artificial Intelligence 4.0* program strives to nourish both academic research and businesses based on AI. One measure for implementation is the Finnish Center for Artificial Intelligence (FCAI) established by Aalto University, University of Helsinki, and VTT Technical Research Centre of Finland. A community of experts involving 60 professors and 300 researchers, FCAI works in research, training and fostering linkages between the private and public sectors. It has been granted flagship status by the Academia of Finland. Adoption of AI solutions is promoted through the establishment of Finland's AI Accelerator (FAIA). It functions as a hub at the intersection of AI applying organizations and companies providing AI solutions.

The rise and fall of Nokia spawned a lively and versatile ecosystem of IT startups in Finland. The Global Startup Ecosystem Report saw Helsinki leap from #59 in 2021 to #31 in 2022.[59] FAIA estimates that over 400 Finnish startups focus on AI,[60] in addition to more established companies such as Reaktor or Futurice whose revenue comes mostly from other products than AI but who nevertheless are prominent providers of AI solutions.

4.2 Digital Defence Ecosystem

Finland applies an ecosystem approach in order to reinforce defence industrial competitiveness, to cross-pollinate know-how and ideas, to find synergies and leverage funding for key technology development. To this aim, *Digital Defence Ecosystem* (DDE) was launched in January 2022. It strives to connect and synergize Finnish defence industry companies, technology providers including SMEs and start-ups, academia, and other stakeholders. Digital solutions and artificial intelligence feature among the key themes of the DDE.

59 For more information, see: https://startupgenome.com/article/global-startup-ecosystem-ranking-2022-top-30-plus-runners-up (last accessed 10 July 2023)
60 For more information, see: https://faia.fi (last accessed 10 July 2023)

Even if the idea originated partly in the Defence Forces, and the ecosystem was granted Government funding for initial coordination activities, the DDE is essentially industry driven. Founding members include, i.a., VTT and various universities, major Finnish suppliers of defence solutions such as Patria, Insta, Saab and Bittium as well as a variety of companies excelling in dual-use technologies like Reaktor, GIM Robotics and EPEC. Coordinated by XD Solutions, the DDE strives to enhance the capabilities and business growth of Finnish companies and research institutions to strengthen their competitiveness in the global market. The role of the Finnish Defence Forces is to ensure the military relevance of project proposals, provide ideas and guidance for products that correspond to defence capability needs, and potentially contribute expertise and testing sites for projects.

The ecosystem seeks synergies between stakeholders of different sectors, functions, and sizes. Many of the Finnish companies specializing in AI are SMEs. Whereas small companies often lack the experience and resources to fully apply EU tools, the ecosystem can provide expertise, support, and economies of scale.

The DDE can provide participants with a joint channel for developing solutions and optimizing the utilization of both national and international funding instruments, such as the European Defence Fund and NATO Innovation Fund. One specific aim is to leverage the adoption of civilian technologies for defence applications. In this, the DDE synergizes with such international initiatives as the Hub for EU Defence Innovation (HEDI) at the European Defence Agency (EDA) and the Defence Innovation Accelerator for the North Atlantic (DIANA), and could potentially function as a vehicle for their implementation.

4.3 FDF's Matrix Approach: Digitalization Office

How the FDF is organized vis-à-vis artificial intelligence needs to be examined in the broader context of digitalization, of which AI is an essential element. Consistently with the MoD guidelines, FDF launched a cross-cutting *Digitalization Programme* at the joint level in 2020. The programme is updated and complemented frequently, reflecting the fast pace of development. The *Government's Defence Report 2021* highlights the importance of the programme:

> Defence Forces is creating the prerequisites for making use of digitalization and the connected new technologies via its Digitalization Programme. The Programme supports the implementation of new technologies and applications in development programs and projects in a centralized manner.

The possibility of creating a specialized Defence AI Center or Agency was discussed within the defence administration at the time of Finland's EU Presidency of 2019. While that specific idea was eventually rejected, a *matrix-type organization* has been established within the FDF called the Digitalization Office, tasked with coordinating the Digitalization Programme. As cross-cutting issues, digitalization and AI are to be mainstreamed into the planning and sectoral development programs of the FDF. The main overarching objectives of FDF digitalization are capacity building for digitalization and exploiting the value-added of digitalization in the development, maintenance, and use of military capabilities. The programme provides top-down guidelines, plans for capacity building for the development of in-house know-how and draws up a framework ensuring interoperability between services and branches. Eventually, each service and each development programme will come up with their own digitalization solutions and AI applications.[61]

61 Karsikas, "Puolustusvoimien digitalisaatio valmistaa huomisen haasteisiin."

5 Funding Defense AI

5.1 Civilian and Dual-Use

Finland's total R&D expenditure was €7.5bn in 2021, amounting to 3.0% of GDP. While this represents a fair 8.1% increase from the previous year, a lot of work remains to be done if Finland intends to stay on track to achieve the Government's goal that R&D expenditure increase to 4% of GDP by 2030. Private companies are responsible for about two-thirds of the R&D expenditure.[62] It is difficult to estimate the share of AI related R&D since much of it is embedded in projects and programs that may involve AI while not focusing only on it.

A governmental investment package specifically aimed at developing AI was launched in 2018. Channeled through Business Finland, the €200M program finances new AI innovations, development of know-how for AI technologies as well as enhancing public sector efficiency by AI applications. This funding is mainly civilian or dual-use, not military. FCAI runs on a budget estimated at €250M for its flagship period 2019–2026. Moreover, the core budget is complemented by project-based funding, which FCAI and its researchers have been awarded several times e.g., by the Academy of Finland. FCAI director Samuel Kaski obtained the Turing AI World-Leading Researcher Fellowship in 2021.

Even if Finland punches above its weight in AI development, its investments are dwarfed by the global superpowers that fund AI by several orders of magnitude more. And not only are the U.S. and China already in a league of their own, but their AI investments are also growing faster than those of Europe. Finland must therefore find niches of specialty expertise or original ideas for application to remain competitive.

5.2 FDF Funding for AI

The annual R&D budget of FDF is about €50M. Information on how exactly this funding is divided between research topics and projects is not publicly available, but the fact that AI is a strategic priority area and the projects showcased above may give an indication of the order of magnitude of the FDF's research funding for AI.

Another important source of AI funding is embedded in the FDF Development Programs other than research. Their content or budget is not publicly available,

62 Statistics Finland, "Tutkimus- ja kehittämismenoissa 8,1 % kasvu vuonna 2021."

but since the FDF Digitalization Program is implemented via the Development Programs, including AI applications, it is obvious that some portion of the national defence budget is also directed towards AI development projects within these programs. Moreover, national R&D investments are often leveraged by international cooperation projects, especially through the EDF which is becoming more and more prominent.

6 Fielding and Operating Defense AI

The Government's Defence Report specifically highlights the role of C2 systems in the context of digitalization and AI. The Report notes that the Finnish Defence Forces establishes and maintains its own C2 systems and operates them in all domains. The Report stresses that the "development of the command system must facilitate the digitalization of the Defence Forces, as outlined in the Digitalization Programme." Here, a reference is made to the Digitalization Programme of the Defence Forces, which is partially based on the guidelines outlined in the Government-level documents. Moreover, the Defence Report mandates the Defence Forces C2 networks to be expanded to areas most critical to defence operational capacities. In addition to its own networks, a collaboration with the networks of other public and commercial partners is also foreseen.[63]

Specific AI capabilities of the Finnish Ground Forces, Navy and Air Forces have scarcely been publicly discussed. There is ample public information on the currently operational equipment, but no in-depth analysis with sufficient technical detail is available as to the degree of digitalization and application of AI in the current operating systems.

6.1 Army

The Finnish Army has estimated that AI is featured in dozens of applications within their operational systems. AI is most prominently used in areas such as support of planning, processing of geodata, data fusion, virtual assistants and other support functions, expert systems, simulations and wargaming. Other areas of application include machine vision and image recognition, predictive analytics, resource allocation, reporting, and various elements pertaining to unmanned and autonomous systems.

Moreover, unmanned systems with autonomous features exploiting AI are part of the research portfolio of the Finnish Army. One of the reasons for specialized in-house research is to ensure that internationally developed concepts and equipment can be adjusted to conform to the Finnish conditions and particular requirements of the Army.[64]

One successful AI application project that has been partly discussed in public concerns fault data analysis of armored vehicles. The FDF pilot project made use of AI to process maintenance data of armored vehicles to automatize the classification and identification of fault events requiring reparatory maintenance. Initial experi-

63 Government's Defence Report, p. 35–36.
64 Lampinen/Tahkokallio, "Autonomian rooli tulevaisuuden maataistelussa," p. 69.

ments with an untaught commercial off-the shelf AI application produced limited results, but after teaching the AI with case-specific data, followed by human expert evaluation, the AI system achieved an 87% detection level of faults. A number of false negatives persisted at the end of the project: a human expert identified a number of cases that the AI had missed. The AI's accuracy of fault identification was extremely high: it correctly classified 99% of the faults detected.

One key takeaway from the project is that while machine learning may certainly be useful for improving and automating predictive maintenance, achieving a useful level of accuracy requires the algorithm to be taught on specific, relevant data. This teaching process can involve, e.g., creating and refining a rule-based model or using machine learning techniques. In this project, both were explored with promising results, whereas the rule-based model was developed further with a solid performance. The teaching process may require significant resources, so areas of application should be chosen accordingly.

The study also highlighted the need for quality inputs: if the original data was very ambiguous, neither a human expert nor the AI managed to make use of it. The AI can refine and use unstructured and uncategorized data but can't deal with fuzziness any better than humans do. Therefore, maintenance data systems should provide preset, unambiguous structures for inputting data. Moreover, for wider application of AI, the maintenance system should enable reliable search functions for data allowing for workflow automatization, as well as develop a systematic, iterative function able to complete missing terms or correct errors.

6.2 Navy

Application of AI in the materiel currently in use in the Finnish Navy can be found in at least three different kinds of systems. *Battle management systems* necessarily feature some degree of AI, e.g., for gathering and processing sensor information. For instance, Hamina class fast attack ships and Hämeenmaa class mine vessels are equipped with Atlas Elektronik's ANCS combat system.

Fire-and-forget *missiles* and *torpedoes* have a degree of AI for navigation and IFF. Finnish missile boats of the Rauma and Hamina classes are equipped with a tailored version of Saab's RBS15 with inertia and GPS navigation. Hamina and Hämeenmaa class vessels also have the ITO 2004 air defence system equipped with Umkhonto missiles. The system processes sensor information for target acquisition and applies missile on-board inertial navigation and infrared seeker after launch.

Current capabilities of the Navy also include UUVs specialized for mine hunting. The Navy's coastal mine hunter vessels of the Katanpää class are equipped with multiple HUGIN and REMUS UUVs produced by Kongsberg.

The Finnish Navy is about to enter a new era with the ongoing *Squadron 2020* project. The project involves the acquisition of four modern corvettes that will eventually replace seven current vessels to be decommissioned. Construction of the four corvettes takes place in 2022–2026. Almost one half of the €1,2bn budget will be spent on combat systems procured from Saab, consisting of sensors, weapon systems and integrated C2.

6.3 Air Forces

The Finnish Air Forces does not disclose details of how it applies AI in its systems, with the exception of certain projects related to logistics and predictive maintenance of Hornet F/A-18s. Two of these projects are a failure prediction system based on machine learning and a Fatigue Life Analysis neural network model:

- **Machine Learning-Based Failure Prediction ("Early Warning System") in Hornet F/A-18s**
  Commissioned by FDF from the Tampere University of Technology, this project created a fault prediction system based on machine learning to analyze data produced by the fighter jet's equipment. The results have been mostly promising, proving particularly useful vis-à-vis hydraulic actuators where faults develop in a slow, cumulative manner. However, extensive amounts of data are needed to achieve a level of accuracy high enough to reliably justify cost-efficient predictive replacement of equipment. This imposes limitations on the potential areas of application for the prognostic AI system: the most suitable target systems are such that are used frequently enough to yield adequate data and in a regular enough manner. The HN F/A-18s were a good candidate, since their mid-life update introduced a data storage system recording over 40,000 parameters. A single flight could yield ten million data points. These were subsequently preprocessed to filter out irrelevant and highly classified data, yielding a sanitized and more manageable data flow specifically relevant for fault analysis. These types of analysis tools are foreseen to be a significant potential aid to maintenance decision-making for several platforms in the near future.

- **Neural Network Based Fatigue Life Monitoring**
  As part of the Finnish Air Force's Hornet Aircraft Structural Integrity Program, a neural network model was created by Patria simulating the structural stress-

es of the F/A-18s using recorded flight data. The model was compared and taught against direct physical strain gauge measurements from two aircraft, with the aim of reaching and adequate level of accuracy for predicting fatigue life for the rest of the 60-strong fleet of F-18s. The Structural Integrity Program started with the creation of a computational model of the HN F/A-18, superimposed with an aerodynamic model, enabling the simulation of specific stresses impacting the aircraft during flight. The virtual models enabled calculating which points in the structure of the aircraft would be most critical. Next, an Onboard Load Monitoring (OLM) system was installed in two HN F/A-18s, which allowed physical measurement of stresses, with a focus on the critical spots predicted by the simulation models. The two aircraft performed flight missions that were deemed representative of the most typical tasks of the FAF, yielding measurement data on the physical tension. The neural network AI was then taught to produce stresses from the OLM physical measurements, the aircraft flight data and a few engineering parameters. The AI model achieved an error rate of less than 20% compared with direct strain gauge measurements. The accuracy could have been even higher without limitations to sampling rates and stored in flight data.

The neural network-based analysis produces useful and cost-effective data to inform decision-making on aircraft structural integrity of the entire fleet without the necessity to physically measure stresses of each aircraft. It is likely that the next generation fighter aircraft will also apply a similar system of AI based stress and fatigue life analysis.

A generational shift is underway. The capabilities of the Finnish Air Forces are destined to undergo a generational transition with the replacement of Hornet fighters by 64 Lockheed Martin F-35A multi-role fighters. The largest public acquisition in Finnish history at €10bn, the F-35s will be operational in Finland from 2025 onwards. The weaponry with which the F-35s will be equipped involves AMRAAM, Sidewinder, SDB I/II, JDAM-family weaponry, JSM and JASSM-ER. Optimized during the procurement, the weapons package will be adapted to Finland's operating environment, also taking into account latest upgrades to the weapon types.[65]

F-35 was evaluated to be the best candidate with regard to combat capabilities as well as reconnaissance and survival. It is noteworthy that the associated direct and indirect industrial cooperation will potentially be a force multiplier for the FDF's research and development activities in various fields, including defence AI applications.

65 "Lockheed Martin F-35a Lightning II on Suomen seuraava monitoimihävittäjä."

7 Training for Defense AI

7.1 AI Expertise and Education at the National Level

Finnish universities provide a broad and durable array of AI related education. Master's level education is provided covering all the ten dimensions of AI listed in chapter 2. Academic research and know-how also span across all these AI elements. In academic curricula offered, the most prominently featuring area is data analytics offered by almost all universities. Several universities provide tuition in perception and situational awareness, human-machine interaction, machine learning, problem solving and computational creativity, platforms, and robotics. Applied research and applications in companies are found to emphasize data analytics, robotics, and perception.[66]

Finland is a small country but scores well in proportion to its population: between 2003 and 2017, Finland produced 3% of the total volume of European AI patents, but in terms of *per capita*, Finland is second in Europe. During that time, Finnish researchers authored 1,257 academic publications on AI, corresponding to 0.5% of the global volume of published AI research (Finland is less than 0.1% of the global population).[67]

One strength of the Finnish ecosystem is the broad-ranging expertise beyond the core AI technologies. Neighboring technology areas such as signal processing, electronics, edge computing and 6G have been successfully combined with AI, such as in cognitive sensor fusion development at Tampere University.

7.2 Training FDF Staff for Using AI

The need for enhanced education and capacity building for exploiting AI across all areas of defence has been recognized at the strategic level. The need for reinforcing expertise and building research and development capabilities pertains to the whole spectrum of AI elements, ranging from perception and situational awareness to data analytics, cognition, computational creativity and machine learning, from system effects and ecosystems to machine automation, human-machine teaming, ethics and regulation.

Training and education for AI are also at the core of the FDF Digitalization Programme. In-house expertise is being reinforced by supplementary education as well as new recruitments, coupled with procurement of external expertise provided by academia and industries. Since digitalization requires an agile approach

---

66 Ailisto et al., Tekoälyn kokonaiskuva ja osaamiskartoitus – loppuraportti, p. 70.
67 Ailisto et al., Tekoälyn kokonaiskuva ja osaamiskartoitus, p. 28.

rather than acquisition of fully operational products, it becomes more important to train competent procurers than to work out extremely finalized acquisition requirements in great detail.

The NDU is strengthening the role of AI in its curricula, and elements of AI are already incorporated in courses at all levels. AI is also increasingly being explored in theses (Bachelor, Master, General Staff Officer Course), with topics ranging from operational analysis and planning to battle management, from internet of things, Big Data and machine learning to AI applications in specific weapon systems.

7.3 Using AI to Enhance FDF Training

AI can be used specifically to enhance training and education in defence. Digitalization and AI are being used to develop an improved selection process of professional soldiers and other defence staff.[68] Parts of conscription service are also being digitalized with trainings and supplementary materials offered in virtual format. Potential for enhancing this training via AI applications has been identified if not yet widely applied.

One particularly promising field where AI can contribute to enhancing training is simulators. FDF deploys a number of different simulators specializing for different services and functionalities: simulators are used for training of nearly every weapon system. For instance, FDF Ground Forces use live simulators (KASI), virtual battle space simulators (VBS), battle tank training simulators (Steel Beasts) as well as constructive simulators (KESI). These are based on commercial engines tailored with national models and parameters for FDF materiel, troops and the Finnish environment.

The simulator that currently makes the most out of AI is the KESI, specifically designed to train commanders to lead troops. Its AI features provide decision-making support and simulate the operation of those troops that are not under the command of the user, or the troop being trained[69].

All of the simulators generate data that could be exploited for operation analysis and planning. Due to the large volumes of data, harnessing AI for the analysis is a *sine qua non*. Moreover, AI-powered simulation provides potential for upscaling, for example with the use of wargaming extensive exercise campaigns, where AI could assist both in the planning and analysis phases but especially in simulating enemy operation instead of human players.

68 Government's Defence Report 2021, p. 39.
69 Rautio, "Komentaja- ja esikuntasimulaattorin käyttöönotto – monivaiheinen prosessi," p. 117.

8 Conclusion

Finland places AI high on the policy agenda, and there are ample policies guiding the development of military AI in the broader context of digitalization. In the early stages of the digitalization of defence, emphasis has been in administrative and support processes aiming at cost savings. Baby steps are now being taken in the direction of digitalizing actual military capabilities. However, most of those efforts that the FDF has publicly announced are still being made at the level of R&D and pilot projects rather than fielding AI solutions.

In 2022, FDF Chief Digital Officer wrote the "objectives of real digitalization will take it a step further."[70] The next step is using data in a more comprehensive way and developing systems based on use cases. This transformation will be based on advanced data analytics capabilities and requires a paradigm change. Simplistic models of cost-efficiency may need to be left behind as "earlier benchmarks and measurements are not necessarily appropriate for assessing the new situation." Efficiency measurements may not be commensurate, when the benefits are increasingly qualitative. This may imply that AI applications not only help achieve existing capabilities more efficiently, but also pave the way towards completely new ways of operating. Implementation of AI solutions will be an iterative process – no sudden overhaul of systems is attempted. Finland's NATO membership in 2023 is accelerating the shift of emphasis in AI and digitalization efforts from supporting functions towards kinetic engagement, with a particular focus on enhanced joint fires. A potential paradigm change may be underway with the emergence of Data-Centric Security.

FDF acknowledges the central role of data availability and usability for digitalization in general and AI applications in particular. In digitalization processes, special attention is now being paid to enabling the gathering and storing of data in formats that allow for flexible and efficient utilization. Silos between different data systems and organizational branches are a known challenge. A particular hurdle is posed by privacy legislation aimed at data protection: the legal principle is that authorities may only use data for the specific reason it was gathered for. For instance, even though general conscription has yielded databases with millions of data points spanning several decades, these cannot be used for research purposes unless the data is processed through rigorous anonymization. Ownership of data is another key point: when developing AI solutions, FDF should be cautious to retain the using rights for the data that machine learning algorithms are trained on – otherwise the supplier may be granted an unfair advantage over competitors or an unhealthy position vis-à-vis its client. The use of synthetic data could solve some of these challenges.

70 Karsikas, "Puolustusvoimien digitalisaatio valmistaa huomisen haasteisiin."

The administrative model for development and acquisition processes of AI poses a special challenge due to the evolutionary character of machine learning. If the AI application is based on continuous improvement, it may not make sense to acquire it at full capacity. Moreover, such a solution is never finished anyway, but will continue to develop throughout its life cycle. This poses a serious challenge for traditional procurement processes, since the functional requirements may need to be regularly reiterated after the initial acquisition. To some degree, current policies of materiel acquisition may prove to be outdated when it comes to AI, since the prevalent norm is to only acquire fully developed and certified technologies – which may simply not be possible with certain AI solutions. An agile and incremental acquisition model would be more appropriate for AI solutions, but that such a model would require the Defence Forces' organizational culture to tolerate experimentation to a greater extent than is currently the case. Such an agile model would involve building a first version with simple AI functionalities, and moving towards increasing complexity with successive iteration rounds all the while retaining the functions that have withstood testing so far.[71]

Ethics and regulation of defence AI have been recognized as a *sine qua non*, and they have been elaborated by Finnish experts in a fairly comprehensive manner. With a lucid categorization of AI application, it becomes evident that most of defence AI concerns systems other than weapons and is therefore unproblematic. Moreover, for the more problematic area of lethal autonomous weapon systems, a conceptual framework has been proposed that could adequately resolve most issues. A grey area will probably always remain, and here an appropriate level of human involvement is required.

Moreover, the best results will be achieved by combining AI and human judgement, making use of the best characteristics of both. AI can be used for a variety of tasks involving analysis of huge data volumes at superhuman speed and increasing the tempo of the OODA loop, whereas the human would provide mission planning and contextual judgement. AI can take on much of the cognitive workload of the human commander, therefore enabling better decision-making. Indeed, an appropriate use of AI can improve compliance with International Humanitarian Law in various ways, ranging from increased precision of targeting to providing better situational awareness.

AI will play a key role in enabling potential disruptions on the battlefield. One such disruption is already beginning to emerge in the form of remote autonomous systems, which are the subject of intense research and development work in Finland. Autonomous systems could enable completely new ways of fighting, provided that

71 Hemminki et al., "Tekoälyn kehityksellä autonomiaa asejärjestelmiin – mihin pitäisi varautua?," p. 217.

an optimal division of labor between man and machine is inherently embedded in the concepts of operation. The commander of the troop always bears responsibility for decision-making, regardless of whether the troop consists of machines, people, or both. Ideally, the human provides contextual judgment based on situational awareness, defines the mission and its parameters. The machine can play a supporting or implementing role.

Elements for concepts of operation are being discussed involving manned-unmanned teaming. One important point of view is that a "wingman" approach may not be the optimal way to use unmanned assets. If the unmanned platforms focus on supporting the manned aircraft, the mobility of the faster aircraft is limited to that of the slower ones. Stealth capabilities would be only as good as those of the least stealthy member of the swarm. Therefore, it might be more useful to grant the unmanned assets more independence. Drones could be sent in advance to the area of operation, loitering in search of potential targets or commanded to advance so as to trigger the enemy's air defence, followed by other drones tasked with a jamming or target acquisition mission; the role of the manned aircraft would then be to launch a missile from stand-off distance. An analogy is a hunter and a pack of hounds. As long as the hounds are on a leash, the team is inefficient. With the hounds unleashed, they can locate the prey and chase it into the range of a rifle. The decision to use lethal force is made by the human.

One area which could potentially be revolutionized by AI applications is dynamic management of the electromagnetic spectrum. Communications or electronic warfare transceivers may soon be able to provide spectrum situational awareness and autonomously decide which frequency bands to use with tailored ad hoc waveforms. AI and machine learning could enable the system to find spatial and temporal margin of maneuver in the spectrum in such a way that civilian frequencies are not disturbed, blue force C2 is achieved without enemy interference, and enemy communications intercepted or jammed. Applying such systems currently requires a technological leap as well as removing certain regulatory hurdles.

In conclusion, there is an apparent discrepancy between Finland's ambitious AI policies and the careful and very gradual approach implied by the public statements and documents of the defence administration. AI projects that have been publicly discussed seem to cluster around digitalization of administrative and support capabilities as well as low-TRL research. Nevertheless, AI can bring about a disruption when developed in an innovative and efficient manner, even if applied only to supporting functions, situational awareness, tactical and operational analysis, and other means of accelerating the OODA loop. The potential has been recognized, and the next 5–10 years will show whether a real transformation is achieved.

Literature

Aalto, Janne, “Autonomiset aseet ja etiikka”, in: Finnish Defence Forces, Puolustustutkimuksen vuosikirja (Tampere: Finnish Defence Forces, 2022).

Ailisto, Heikki (ed.), Eetu Heikkilä, Heli Helaakoski, Anssi Neuvonen, Timo Seppälä, Tekoälyn kokonaiskuva ja osaamiskartoitus (Publications of the Government’s analysis, assessment and research activities, Prime Minister’s Office, 2018), https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160925/46–2018-Tekoalyn%20kokonaiskuva.pdf (last accessed 10 July 2023)

Ailisto, Heikki, Tekoälyn käsitekartta (Helsinki, 2018), https://tietokayttoon.fi/documents/1927382/2158283/Teko%C3%A4lyn+k%C3%A4sitekartta/a5c4b469-d8ae-4ce1-a5fc-f12981bae796 (last accessed 10 July 2023).

Ailisto, Heikki (ed.), Anssi Neuvonen, Henrik Nyman, Marco Halén, Timo Seppälä. Tekoälyn kokonaiskuva ja osaamiskartoitus – loppuraportti (Helsinki: Publications of the Government’s analysis, assessment and research activities/Prime Minister’s Office, 2019). https://julkaisut.valtioneuvosto.fi/handle/10024/161282 (last accessed 22 February 2023).

Andersson, Christian, “Laykka-AMPGV:n inkrementaalinen kehitysprosessi runkoversio X.2:sta X.3:een sekä kehityksen seuranta kenttätesteillä ja -kokeella”. Master’s Thesis. 2022, https://www.doria.fi/handle/10024/185591 (last accessed 12 June 2023).

Artificial Intelligence 4.0 First interim report: From start-up to implementation (Helsinki: Ministry of Economic Affairs and Employment, 2021), https://julkaisut.valtioneuvosto.fi/handle/10024/163042 (last accessed 10 July 2023).

Finland, Estonia, France, Germany, and the Netherlands, “Digitalization and Artificial Intelligence in Defence”, Food for Thought Paper for EU Member States, 17 May 2019. Unpublished.

Finland, “Considerations on the appropriate level of human involvement in LAWS”, Food-for-thought paper by Finland for UNCCW GGE, June 2020. Unpublished.

Finland, “Elements for possible consensus recommendations”, contribution to UNCCW GGE, June 2021. Unpublished.

Finnish Defence Forces, Puolustustutkimuksen vuosikirja (Tampere: Finnish Defence Forces, 2022), https://puolustusvoimat.fi/documents/1951253/2815786/Puolustustutkimuksen_vuosikirja2022.pdf (last accessed 10 July2023).

Government’s Defence Report (Helsinki: Publications of the Finnish Government 2021). http://urn.fi/URN:ISBN:978–952–383–852–9 (last accessed 10 July 2023).

Harju, Jukka, “Puolustusvoimat testasi maarobottia, josta voisi tulla suomalaissotilaiden taisteluapulainen 2030-luvulla”, Helsingin Sanomat, 31 March 2022, https://www.hs.fi/kotimaa/art-2000008720073.html (last accessed 10 July 2023)

Heiskanen, Mikko, Puolustusvoimien näkökulmia tekoälyyn, presentation at a MATINE seminar 21 December, 2018, https://www.defmin.fi/files/4463/AI_Roadmap_MATINE_JULK.pdf (last accessed 22 February 2023)

Hemminki, Petteri, Kai Virtanen, Kimmo Halunen, “Tekoälyn kehityksellä autonomiaa asejärjestelmiin – mihin pitäisi varautua?”, in: Kaarlakoski et al., Sotataloustietoutta XI (2021), pp. 210–235.

Jylhä, Juho, Marja Ruotsalainen, Minna Väilä, Juho Uotila, Markku Åkerblom, Henna Perälä, “MATINE-hanke 2500M-0133: Hajautetun järjestelmän ja sensorifuusion parviälykäs ohjaus (2021–2022)”, https://www.defmin.fi/files/5549/1330_MATINE_2500M-0133_Tutkimusseminaari_2022_Patria_Jylha.pdf (last accessed 17 July 2023).

Kaarlakoski, Miina, Pekka Koistinen, Harri Jalonen, Anssi Keinänen, Harriet Lonka, Valdemar Kallunki, Sotataloustietoutta XI: Sotatalous 2020-luvulla (2021). https://bin.yhdistysavain.fi/1584898/5C8xfmHlDz1thiIvjrBm0WhlRi/Sotataloustietoutta_XI_verkkojulkaisu.pdf (last accessed 10 July2023).

Kallinen, Kari, “Kognitiivinen sodankäynti”, in: Puolustustutkimuksen vuosikirja (Tampere: Finnish Defence Forces, 2022).

Kalliomaa, Mika, “Eettinen tietoisuus vastuun keskiössä”, Ilkka, 23 July 2019.

Karsikas, Jarkko, “Puolustusvoimien digitalisaatio valmistaa huomisen haasteisiin”, 8 August 2022,https://puolustusvoimat.fi/blogi/-/blogs/puolustusvoimien-digitalisaatio-valmistaa-huomisen-haasteisiin (last accessed 10 July 2023).

Kosola, Jyri, “Teknologia 2035+”, in Rantapelkonen, Tuleva sota – Tulevaisuuden sodan tulevaisuus (2018), pp. 44–83.

Kosola, Jyri, “Robottiaseet herättävät keskustelua”, Sotilasaikakauslehti 1/2020, pp. 72–78.

Kosola, Jyri, “Maasodankäyntiä vuonna 2020”, Sotilasaikakauslehti 2/2020, pp. 80–86.

Kosola, Jyri, “Naton teknologianäkymiä vuoteen 2040”, Sotilasaikakauslehti 4/2020, pp. 74–78.

Kosola, Jyri, “Sodankäyntiä muuttavat teknologiset ilmiöt”, Sotilasaikakauslehti 6/2020, pp. 70–74.

Kosola, Jyri, “Palapelin rakentelua vai peliä mosaiikilla”, Sotilasaikakauslehti 2/2021, pp. 74–78.

Kosola, Jyri, “Paradigman muutos”, Sotilasaikakauslehti 4/2021, pp. 60–66.

Kosola, Jyri, “Hyvä – paha digitalisaatio”, Sotilasaikakauslehti 7/2021, pp. 64–70.

Kosola, Jyri, Presentation at ASDA seminar, 22 November 2022, unpublished.

Lampinen, Timo and Tatu Tahkokallio, “Autonomian rooli tulevaisuuden maataistelussa”, in Puolustustutkimuksen vuosikirja (Tampere: Finnish Defence Forces, 2022).

“Lockheed Martin F-35a Lightning II on Suomen seuraava monitoimihävittäjä,” Ministry of Defence, 10 December 2021, http://www.defmin.fi/ajankohtaista/tiedotteet_ja_uutiset/tiedotearkisto/tiedotteet_2021/lockheed_martin_f-35a_lightning_ii_on_suomen_seuraava_monitoimihavittaja.12334.news (last accessed 10 July 2023).

Strategic Guidelines for Developing AI Solutions (Helsinki: Ministry of Defence, 2020), https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162372/Strategic_guidelines_for_developing_ai_solutions.pdf (last accessed 10 July 2023).

Puolustushallinnon materiaalipoliittinen strategia (Helsinki: Ministry of Defence, 2023). http://urn.fi/URN:ISBN:978–951–663–269–1 (Last accessed 26 May 2023).

Nieminen, Mika, Petteri Hemminki, Tapio Haapamäki, Christian Andersson, “Autonomia taistelukentällä – tulevaisuusorientoitunut tutkimus”, in Puolustustutkimuksen vuosikirja (Tampere: Finnish Defence Forces, 2022).

Rantapelkonen, Jari (ed.), Tuleva sota – Tulevaisuuden sodan tulevaisuus (Helsinki: National Defence University of Finland, 2018).

Rautio, Samu, “Komentaja- ja esikuntasimulaattorin käyttöönotto – monivaiheinen prosessi”, in Puolustustutkimuksen vuosikirja (Tampere: Finnish Defence Forces, 2022).

Russell, Stuart J. and Peter Norvig (eds.), Artificial Intelligence: A Modern Approach (Hoboken: Pearson, 2021).

State of AI in Finland, 2020 (Helsinki: FAIA, 2020), https://faia.fi/market-research/ (last accessed 10 July 2023).

Statistics Finland, “Tutkimus- ja kehittämismenoissa 8,1 % kasvu vuonna 2021”, 27 October 2022, https://stat.fi/julkaisu/cktwmucpk415n0b04ft95vmy6 (Last accessed 10 July 2023).

Tiilikka, Jari, Jani Ristimäki, Santtu Kukkonen, Timo Anttila, “Taistelija-hanke”, in: Kaarlakoski et al., Sotataloustietoutta XI (2021), pp. 123–131.

Tikka, Jarkko and Tuomo Salonen, “Practical Experience of Neural Network Based Fatigue Life Monitoring”. Paper presented at ICAF symposium (2015).

Defense AI Observatory Studies

23|16 Sami O. Järvinen, Cautious Data-Driven Evolution. Defence AI in Finland

23|15 Inbar Dolinko and Liran Antebi, Embracing the Organized Mess. Defense AI in Israel

23|14 Alastair Finlan, A Fertile Soil for AI? Defense AI in Sweden

23|13 John Lee, "Overtaking on the Curve?" Defense AI in China

23|12 Heiko Borchert, Torben Schütz, and Joseph Verbovszky, Master and Servant. Defense AI in Germany

23|11 Katarzyna Zysk, High Hopes Amid Hard Realities. Defense AI in Russia

23|10 Yvonne Hofstetter and Joseph Verbovzsky, How AI Learns the Bundeswehr's "Innere Führung." Value-Based Engineering with IEEE7000™-2021

23|09 Robert C Engen, When the Teeth Eat the Tail: A Review of Canada's Defence Artificial Intelligence

23|08 Çağlar Kurç, Enabling Technology of Future Warfare. Defense AI in Turkey

23|07 Lauren A. Kahn, Risky Incrementalism. Defense AI in the United States

22|06 Yvonne Hofstetter, Wie KI Innere Führung lernt. Wertbasierte Technik mit IEEE7000™-2021

22|05 Andrea Gilli, Mauro Gilli, and Ivan Zaccagnini, Exploring the Benefits of a New Force Enabler: Defense AI in Italy

22|04 Kenneth Payne, Bright Prospects – Big Challenges. Defense AI in the United Kingdom

22|03 Heiko Borchert, Christian Brandlhuber, Armin Brandstetter, and Gary S. Schaal, Free Jazz on the Battlefield. How GhostPlay's AI Approach Enhances Air Defense

22|02 Peter Layton, Evolution not Revolution. Australia's Defence AI Pathway

21|01 Heiko Borchert, Torben Schütz, Joseph Verbovszky, Beware the Hype. What Military Conflicts in Ukraine, Syria, Libya, and Nagorno-Karabakh (Don't) Tell Us About the Future of War

DAIO Defense AI Observatory

www.defenseai.eu