Strategic guidelines for

DEVELOPING AI SOLUTIONS

Puolustusministeriö
Försvarsministeriet
Ministry of Defence

CONTENTS

Publisher: Ministry of Defence, Finland 2020

Layout: Tiina Takala

ISBN: 978-951-663-099-4 print

ISBN: 978-951-663-100-7 pdf

1. INTRODUCTION

There are a number of different definitions for the term **artificial intelligence**. According to a clear definition, “AI enables machines to perform tasks for which human intelligence has previously been required”.

At the moment, however, AI implementations are still very specific, performing only very strictly limited, predetermined tasks. It would often be more appropriate to use the term **support intelligence** instead of **artificial intelligence**. Artificial intelligence that is similar to human intelligence or capable of human consciousness is not expected to emerge in the next few years. AI performs best in tasks the human brain cannot cope with. For example, when the amount of information or the required processing speed is too high, or an analysis independent of human variables is needed.

Global digitalisation and, as a result, the development of AI applications have strongly shaped the world in which we live. Artificial intelligence technologies make one of the most important digital performance leaps of our time possible. Russia, China, the USA, EU countries and a number of large companies are investing heavily in the development of artificial intelligence. They build capabilities that utilise AI and collect data that serves as fuel for these systems. Finland and the defence administration are not separate from this international development.

In order for Finland to retain its credible defence capability, our AI and digitalisation capabilities must be developed. Traditionally, defence administration has developed its capabilities by purchasing ready-made solutions. However, artificial intelligence and digitalisation require both the development of own expertise and the search for new partners. A technical infrastructure that serves the whole is needed, building on the storage and safe distribution of data, development of AI applications and implementation to production. Creating such infrastructure requires modern and agile software development routines and tools.

Despite the technological background, the key themes of performance development are related to governance and competence.

The defence administration has drawn up strategic guidelines for the development of artificial intelligence that support the building of capabilities. The guidelines consist of the administrative prerequisites for the activities, the requirements for competence and the technical capacity to implement them.

2. Strategic steering for developing AI capabilities

Artificial intelligence was one of the key themes in the joint initiatives on defence capability development during Finland's 2019 EU Presidency (***Digitalization and Artificial Intelligence in Defence***). Artificial intelligence is brought up a number of times in the 2019 Government Programme, too. Already in 2017, the AI programme of the Ministry of Employment and the Economy set an ambitious target to make Finland one of the leading countries in the application of AI.

Many statements, research papers and guidelines on autonomous weapon systems and the use of AI as part of weapon systems (***Lethal Autonomous Weapon Systems, LAWS***). These include the EU Parliament, 2018; Finland and Estonia 2018; and the UN CCW GGE, ***Convention on Certain Conventional Weapons, Group of Governmental Experts, 2019***).

Globalisation, post-Cold War transformation, anti-terrorism war and digitalisation have significantly altered the field of international threats. Activities in this multidimensional field will take place more and more quickly and focus not only on the traditional land, air and sea dimensions but also on space, cyber and information dimensions and the human mind. Anyone who is able to harness the information to their service the fastest is at the forefront of the global competitive environment.

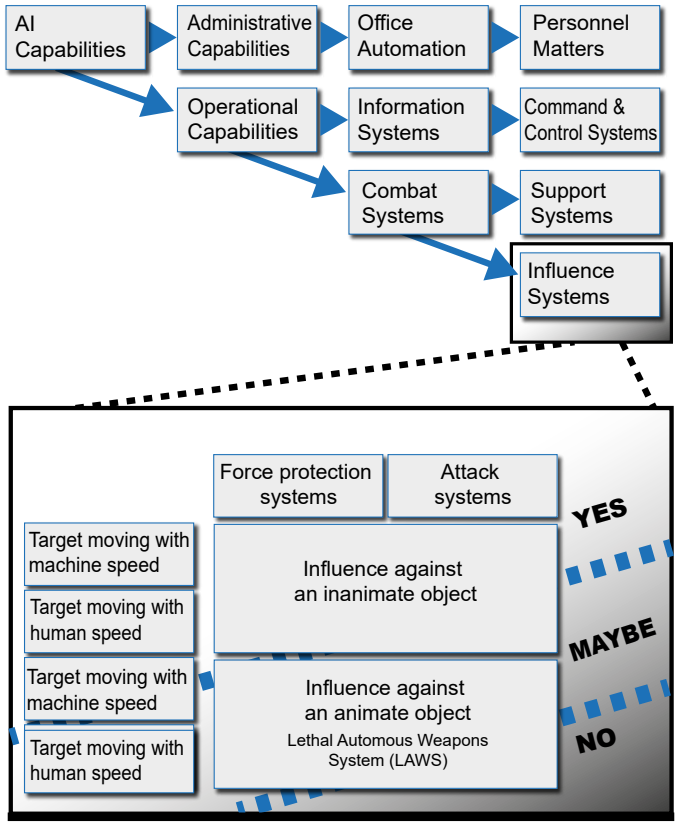
The amount of data has increased exponentially, which means that more efficient methods are needed to deal with it. Rapid development of AI capabilities is the only way to maintain the balance of the current defence capability in relation to national threats.

3. Areas of AI capability

3.1 Administrative prerequisites

The administrative prerequisites for utilising artificial intelligence consist of ethics and legislation, management perspectives, communications, procurement and resourcing. In order to develop artificial intelligence capabilities appropriately, the administrative prerequisites must be adequately met.

In all development of AI capabilities, the defence administration undertakes to comply with international law and ethical obligations that are binding on the administrative branch. As the trends in national and international regulation have a significant impact on the capability of the Defence Forces to carry out their statutory duties, the defence administration is actively involved in drawing up them. National or international legislation must not prevent the development of ethically acceptable, necessary and appropriate solutions based on artificial intelligence.



Picture: The majority of different AI applications are on a very solid ethical and legal basis. Naturally, the same good governance practices must be taken into account in their use and development as in other work related to personal data, privacy protection and transparency of decision-making. Applications in the grey area require a situation-specific review, and only LAW systems that remain in the completely black area require in-depth legal and ethical consideration.

Defence administration does not practise self-regulation, which is stricter than what is required by laws and regulations. Defence administration develops artificial intelligence capabilities under the same conditions as others. Further challenges are created by actors that do not comply with international regulations, so the defence administration must be able to prepare for such threats, too.

AI solutions are based on good governance. The defence administration has the necessary legal understanding of what and how data can be collected, stored and combined. There are clear and complete administrative and legal practices for the connection, collection and processing of new data.

There is a shared understanding within the defence administration of the capabilities that digitalisation and artificial intelligence must achieve. The senior management in the administrative branch is committed to these objectives. Digitalisation and artificial intelligence must release resources from administrative work to operational work and increase operational performance in both normal and emergency conditions. Internal communications and training will ensure that there is an adequate understanding of artificial intelligence at different levels of the organisation.

Different aspects of digitalisation (e.g. cyber, artificial intelligence, cloud computing services and information) have drawn up their own strategic plans that are compatible and in line with each other. Due to the rapid technological development, the plans will be updated regularly.

There is a lively public debate on threats and opportunities related to artificial intelligence. Technology is subject to a wide range of assumptions and expectations, and the debate is often conducted without an in-depth understanding of the basis for technology. The defence administration takes actively part in the debate. There are very few ethically questionable applications compared to the total number of applications.

Artificial intelligence can also be used to reduce human suffering. It will help to cause minor collateral damage and fewer military and civilian casualties in a crisis situation.

As in digital development projects in general, the acquisition, planning and implementation of AI capabilities is agile. The purchase process differs from the purchase of material performance, and the Procurement Act supports agility well. In addition, agility will be accelerated through training and models that serve as examples.

Funding must also be agile in order for the research, product development and deployment of new technologies to succeed within the timetable set out in the performance targets. The primary aim of the procurement is to buy a capacity that produces the desired capability (for example, the right team), not so much a product or equipment (for example, predefined software)..

3.2 Competence

AI capabilities require external expertise both within the defence administration and from the partner network. Different skills profiles are needed for different tasks. In addition, Artificial Intelligence expertise must be widely divided into different parts of the defence administration.

The AI expertise of the Defence Forces personnel will be developed and the AI expertise of conscripts and reservists will be utilised systematically. New staff will be recruited for expert duties and current staff will be further trained.

The Defence Forces have a network of AI partners consisting of companies, research institutes and academic communities. The network integrates the domestic and international actors whose capabilities are needed to achieve the objectives. The partners will be assessed and integrated into the network through a uniform mechanism.

The tasks for which the expertise of the partners can be used and where expertise should be found in the Defence Forces have been identified as the basis for cooperation. Together with its network of partners, the Defence Forces will develop a systematic and active transfer of expertise within the organisation. The Defence Forces must have the capability to develop and maintain AI solutions requiring the highest level of concealability independently.

In the defence administration, the network's co-operation is carried out by designated persons.

As outlined in the ***Strategic Guidelines for Developing Cyber Defence*** (2019), cooperation on artificial intelligence will also be developed in cooperation with educational institutions. The development of educational programmes and courses in educational institutions will be supported so that they serve the needs of continuing AI training, improve the recruitment base, maintain a high level of national AI competence and promote the monitoring of the development of AI competence areas.

3.3 Implementation capability

The implementation of AI capabilities requires the availability of data (collecting, combining and processing data and making it technically available), AI technologies and technical infrastructure (calculation environment, storage, data transfer and support systems) in which applications are implemented. Such an entity also serves other digitalisation projects in the administrative branch.

Artificial intelligence solutions are built on data generated by the digital world at an accelerating pace. Various personal data registers, for example, accumulate date which is stored in databases as a by-product of activities and processes. Data collection is often the goal; especially in intelligence gathering the continuous collection and analysis of data is at the core of activities. Above all, data collection and management require focus and prioritisation. The aim is to identify which data must be available in the defence administration. The necessary processes and technical solutions for data collection, storage, availability, enrichment and analysis exist. This package will be reviewed regularly and, if necessary, amended.

The defence administration must have an up-to-date technical infrastructure to run AI applications. The technical infrastructure enables the development of models and their implementation in production with the technology required. The entity is built on centralised common resources and local capabilities. Export of AI solutions to production may mean, for example, an office intelligence application serving the entire administrative branch on a centralised server, a technical interface sharing the results of an analysis, or support intelligence in rolling stock or in a fighter's equipment. AI solutions require monitoring and must be able to be updated and further developed safely.

As to capability development and maintenance, technological development will be taken account of in a proactive and agile manner, and infrastructure will be updated iteratively, when necessary. Technological solutions must be made in such a way that they support international cooperation and the objectives of the partnership programmes.

The solutions must be of a sufficiently general nature so that optimal technology can be applied in different situations. A significant proportion of AI solutions are built on open source programming libraries or they utilise pre-instructed models (for example, different image recognition models and modern common language models), either as such or modified according to usage cases. Commercial AI products also have a role to play. For these products, it must be ensured that they are easily integrated into other systems. Technological environments will be developed in such a way that they can make use of both new, openly available technologies and commercial solutions in narrow specific fields.

4. Strategic guidelines

1	**Coordinated strategic guidelines:** The strategic level of defence administration plans for all aspects of digitalisation are compatible and aligned. The plans will be updated regularly.
2	**Agility and case-based ownership:** Research, development and maintenance of AI capabilities will be procured and resourced in a agile manner in order to realise the performance potential of rapid technological development. Agility is supported by training. The ownership of AI solutions and the data used in them belongs to the owner of the activity or process in the organisation.
3	**Active development of skills:** In developing AI capabilities, critical competences are secured through recruitment and staff training. An active network of AI partners including companies, research institutes and the academic community will be created for the defence administration, and skills will be actively developed with the network.
4	**Availability of data and flexible technical solutions:** The defence administration identifies which data must be available. The necessary processes will be carried out to manage the data. The defence administration will develop an up-to-date technical infrastructure for the promotion of AI applications. Data, processes and infrastructure are updated iteratively.
5	**Legality, ethics and open discussion:** The defence administration complies with international legal and ethical obligations that are binding on the administrative branch in the construction and use of artificial intelligence and participates actively in the drafting. The defence administration actively participates in public discussion on the threats and opportunities of AI.

5. Working group

A working group was set up from key personnel in the defense administration, with the consulting company Reaktor as a partner. The content was created in workshops and other regular meetings. Reaktor interviewed important stakeholders and studied external research and literature.

Members of the working group:

Teemu Anttila, chairman.

Pekka Appelqvist

Rauno Kuusisto

Joona Lapinlampi,

Antti Lehtisalo

Juha Martelius

Pentti Olin

Tero Solante

Antti Tunkkari

Markku Vihersalo

Ministry of Defence, Finland 2020