UNIVERSITY
OF TURKU

NEW BRAINS FOR THE DEFENCE SYSTEM

Systematic view on the Finnish Defence Forces on the edge of Artificial Intelligence revolution

Master of Science Thesis
University of Turku
Department of Future Technologies
Computer Science
2020
Petteri Hemminki

Supervisor:
Jukka Heikkonen

UNIVERSITY OF TURKU
Department of Future Technologies

Petteri Hemminki: New Brains for the Defence System - Systematic view on the Finnish Defence Forces on the edge of Artificial Intelligence revolution

Master of Science Thesis, 54 pages, including 4 pages of appendices
Computer Science
April 2020

There are about 3,5 billion smartphones in the world, and all users can use applications based on the research of Artificial Intelligence. The rapid expansion of this research to the new areas creates both new threats and possibilities for the defence systems in the future. The Finnish Defence Forces is obligated to plan, implement, and maintain adequate military capabilities for all risk dimensions and an essential question is raised, how to prepare the whole defence system for the future development of Artificial Intelligence as an emerging research area.

To answer this question, the Soft System Methodology is chosen for the main method of this study. This methodology is suitable for the future studies, when the area of study is complex, organized, self-regulating, dynamic and in interaction with its environment. This provides a needed holistic approach to the defence system along with a foresight perspective. The other method, document analysis is focusing on the open sources and used to study the characteristics of the defense system and the history of technological development. The third method, deductive reasoning, is used especially in model creation and risk analysis.

As a result, this study presents five recommendations for the organization:

- the organization should increase the intensity of collecting data
- the organization should improve the capability to store and share data
- the organization should boost the training of agile methods with the experimental projects
- the organization should tune-up organizational culture to match the future
- the organization should keep on monitoring the development of AI

The research results can be summarized in the following conclusion: it is important to choose the role we want to play in this potential Artificial Intelligence revolution - today's decisions matter the most for the future.

Keywords: Artificial Intelligence, Soft System Methodology, defence, system, future

TURUN YLIOPISTO
Tulevaisuuden teknologioiden laitos

Petteri Hemminki: Uutta älykkyyttä puolustusjärjestelmälle – Järjestelmänäkymä Suomen Puolustusvoimista lähestyttäessä tekoälyn vallankumousta.

Pro Gradu, 54 sivua, sisältäen yhden nelisivuisen liitteen
Tietojenkäsittelytieteet
Huhtikuu 2020

Maailmassa on noin 3,5 miljardia älykännykkää, joissa voidaan käyttää applikaatioita, jotka perustuvat tekoälytutkimukseen. Tämän tekoälytutkimuksen nopea leviäminen uusille alueille luo uusia uhkia ja mahdollisuuksia puolustusjärjestelmille tulevaisuudessa. Suomen Puolustusvoimilla on velvoite suunnitella, rakentaa ja ylläpitää riittäviä sotilaallisia suorituskykyjä kaikkia uhkaulottuvuuksia varten, mikä herättää kysymyksen siitä, miten koko puolustusjärjestelmän tulisi varautua tulevaisuuteen nopeasti kehittyvän tekoälytutkimuksen takia.

Tässä tutkimuksessa esitettyyn kysymykseen vastataan pehmeän systeemimetodologian avulla, joka on valittu tutkimuksen päämetodiksi. Se soveltuu tulevaisuuden tutkimuksen menetelmäksi, kun tutkittava alue on monimutkainen, organisoitu, itsesäätelevä, dynaaminen ja vuorovaikutteinen ympäristönsä kanssa. Tämä mahdollistaa puolustusjärjestelmän lähestymisen kokonaisvaltaisella ja tulevaisuuden näkökulman säilyttävällä tavalla. Toinen käytettävä metodi, avoimiin lähteisiin perustuva kirjallisuustutkimus, keskittyy tutkimuksessa puolustusjärjestelmän ominaispiirteisiin ja teknologisen kehityksen historiaan. Kolmatta metodia, deduktiivista päättelyä, käytetään erityisesti mallien luomisessa ja riskien analysoinnissa.

Tutkimustuloksena esitetään organisaatiolle seuraavia suosituksia:

- organisaation tulisi panostaa datan keräämisen tehokkuuteen
- organisaation tulisi parantaa kykyä tallentaa ja jakaa dataa
- organisaation tulisi tehostaa harjaantumista ketteriin menetelmiin kokeiluluonteisilla projekteilla
- organisaation tulisi virittää organisaatiokulttuuriaan vastaamaan tulevaisuutta
- organisaation tulisi jatkaa tekoälyn kehittymisen seurantaa

Tutkimustulokset voidaan tiivistää seuraavaan johtopäätökseen: on tärkeää päättää, missä roolissa haluamme kohdata tulevaisuudessa mahdollisen tekoälyn vallankumouksen - tämän päivän päätöksillä on kaikkein tärkein merkitys tulevaisuuden kannalta.

Avainsanat: tekoäly, pehmeä systeemimetodologia, puolustus, järjestelmä, tulevaisuus

Table of contents

List of figures

List of tables

Acronyms and abbreviations

AI	Artificial Intelligence
BC	Before Christ
C4	Command, Control, Communications and Computers
CATWOE	Customers, Actors, Transformation process, Worldview, Owners and Environmental constraints
DoD	Department of Defence
e.g.	exemli gratia, for example
etc.	et cetera, and the rest
FDF	Finnish Defence Forces
GAI	General Artificial Intelligence
IPR	Intellectual Property Rights
IQ	Information Quality
J2	Intelligence
J4	Logistics
J6	Command and Control
MoD	Ministry of Defence
OODA	Observe, Orient, Decide, Act
RD	Root Definition
RS	Risk Score
SSM	Soft System Methodology

1 INTRODUCTION

"The future is not set, there is no fate, but what we make for ourselves"- Terminator 2

The national defence system of Finland is an extraordinarily complex and dynamic system of systems. This overall system is facing an enormous challenge - the development of Artificial Intelligence and its consequences for the whole defence system.

In this thesis, Artificial Intelligence (later AI) is considered as a wide and evolving research field, that enables new kinds of applications and embodiments including the system development of military technology. This development is neither limited just to a couple of current technology fields like speech recognition, computer vision or natural language processing[1] nor some individual system – it concerns the whole defence system. How to cover this broad and complex entity which is evolving through the time? To solve this question, the Soft System Methodology is chosen for the main method, but also other aspects of system thinking are also considered. This thesis covers essential steps of the Soft System Methodology.

The chosen time perspective is 2020-2040. Twenty-years' timeline is quite a long period to predict the development phase of AI technology, which is one of the most rapidly evolving research areas nowadays. Despite this rapid development, one major assumption is stated and that is the "fact" that General Artificial Intelligence (later GAI) cannot be achieved during this time. GAI is an overwhelming machine or artifact capable to successfully perform any intellectual task that a human being can. Even without achieving this GAI, the development in several narrow areas can create cascading effects on to the existing defence system.

The main method is based on the fundamental thoughts of future research[2]. The approach to this subject is objective and open minded, based on the principle, that we can influence the future by our own actions – but only, if we can predict and understand the implications of AI. Professor Yuval Harari has said that "We should never underestimate human stupidity"[3] and in the wrong hands, AI will be the worst tool or the most horrible weapon especially if the "hands" belong to the self-aware defence system. Future defence systems like fictitious Skynet[4] can become self-aware and not just in science fiction novels or Hollywood movies. This thesis should not be considered as a guide for weaponizing Artificial Intelligence – it is merely a philosophical study considering how today's decisions and activities with Artificial Intelligence affect the future development of the Finnish Defence System.

1.1 Aim and research questions

The purpose of this thesis is to provide a common framework with a systematic view of the future development of Artificial Intelligence in the Finnish Defence Forces. This study aims to generate knowledge for strategic decision making in order to guide the development and implementation of Artificial Intelligence in the next 20 years. This study focuses on the development of military capabilities, but the results can be applied to any organization using a process-based operating model.

This study is based on the following vision:" In the year 2040 functions at all the different levels of the Finnish Defense System are supported by artificial intelligence applications including support to the decision-making and controlled use of autonomous systems."

The main question of this study is:" How to prepare the Finnish Defence System for the future development of Artificial Intelligence?" The main question of this study is divided into five sub-questions:

1.) Why the Finnish Defence System should prepare for the development of Artificial Intelligence?
2.) What is the systematic view on the Finnish Defence system in the eyes of AI?
3.) How to approach the future systematically?
4.) How to define essential future AI opportunities and threats?
5.) What recommendations should be considered in today´s decision making?

1.2 Methods

The main method of this study is the Soft System Methodology. It is a structured way of thinking combining principles of systems engineering and organizational issues by Peter Checkland[5]. The choice of this research method allows a comprehensive approach to the complex system together with future foresight. The main method is supported by a documentary analysis because documents can reveal a great deal about the people or organization that produced them and the social context in which they emerged[6]. Deductive reasoning is used especially in model creation and risk analysis.

1.3 Limitations and restrictions

There are three major limitations in this study that could be addressed in future research. First, the study is focused on the future defined by the vision presented earlier. The future is unknown, and the created vision is just one description of the possible future. This vision is not official, and it has no real connections to the strategic work of the Finnish Defence Forces (later FDF). Second, this research is based on some vital assumptions considering the future – the duties of the Finnish Defence Forces

and main processes remain similar in the future. Third, all the steps of the Soft System Methodology cannot be covered in this study, because they need real activities and resources from the FDF.

One additional restriction in this study is the chosen technique in collecting data and especially documents. All the documents in this study are part of the public domain and accessible. This choice of leaving the restricted documents out of scope is deliberate and may hamper the accuracy of the research results but staying on the general level with the chosen main method is the experimental part of this study and it enables sharing and further open discussion of this research. Similarly, this research report does not include information on the current state of the Finnish Defense Forces or its future plans. The purpose of this thesis is to support strategic decision making by providing practical recommendations concerning the future of Artificial Intelligence.

1.4 Conceptual framework

The following conceptual framework is created to describe the essential key factors of this study and the relationships between them visually. The aim of the study is to create recommendations, which increase interactivity between future development of military capabilities and Artificial Intelligence.

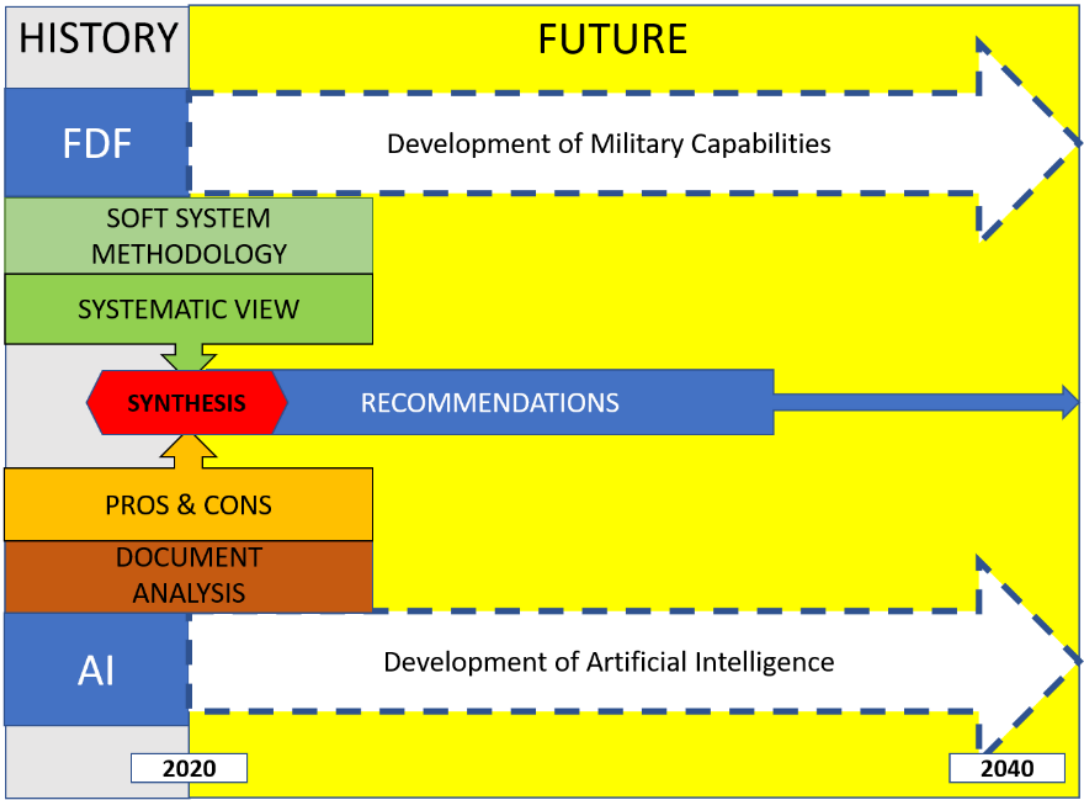

Figure 1: Conseptual Framework

2 BACKROUND OF THE SYSTEM

This chapter presents the organization, its duties, main processes, capabilities, risk environment and the need for system thinking in this research. It also reveals external and internal threats that are potential due to the future development of artificial intelligence.

2.1 Brief organizational overview

Finnish Defence Forces is a governmental organization whose duties and responsibilities are described in the Finnish legislation[7]. It is a task-oriented organization and the stationary duties are followed:

- The military defense of Finland,
- Giving support to other authorities,
- Participating in activities stated in Article 222 of the Treaty on the European Union
- Participating in international military crisis management and in military duties.

FDF personnel in the peacetime is about 12000 and the annual number of conscripts is about 280008. Most of the personnel are in the three branches – army, navy and air force that are described below. Total wartime amount of personnel is about 300 000 with reservists.

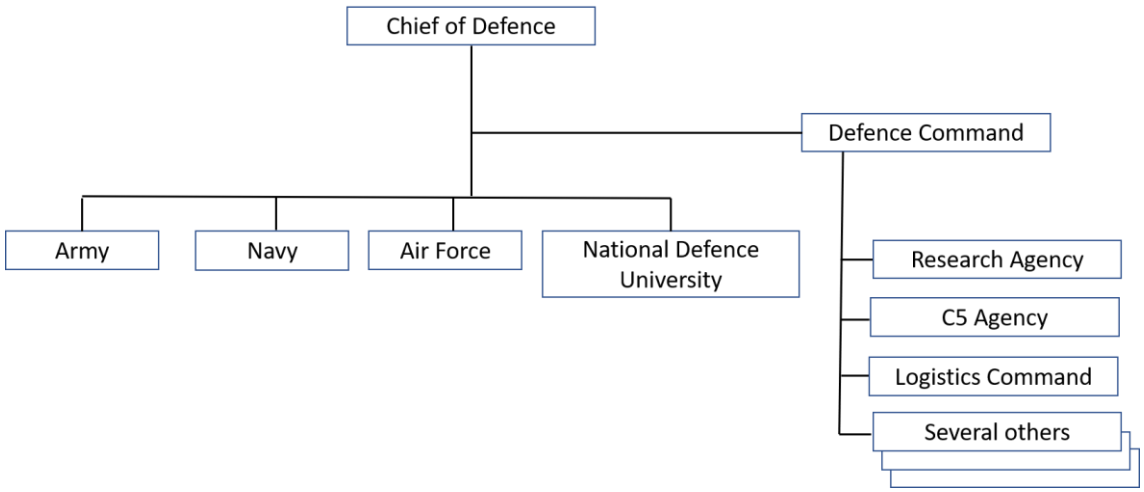

Figure 2: Organization of the Finnish Defence Forces

Main processes of the FDF are[9]:

- capability planning and development
- capability building and maintenance
- readiness control and use of capabilities
- service activities

In the defence system, there are several subsystems. Some of the subsystems are so-called “joint systems” and they are used in all branches and higher echelons. Typical joint systems are logistics, communications and intelligence systems. Some systems are specific for a certain branch - for example army and the main battle tank or navy and battleship connections. There are several hundred different subsystems and all these subsystems are connected to each other and together they provide whole defence capability. The FDF maintain and develop this capability to perform tasks defined by the foreign, security and defence policy of Finland’s political leadership.

2.2 Capabilities and Gaps

Capability is a very essential term in military use. There are several ways to arrange capability elements and the following capability system model DOTMLPF-P is just one way to describe the complexity of military capability[10]. DOTMLPF-P stands for:
- **D**octrine: the way we fight (e.g. offence, defence, operational principles)
- **O**rganization: how we organize to fight (e.g. creating units and task forces)
- **T**raining: how we prepare to fight tactically (basic training to advanced individual training, unit training, joint exercises, etc).
- **M**aterial: all the “stuff” necessary to equip our forces (weapons, spares, test sets, etc that are “off the shelf” both commercially and within the government)
- **L**eadership and education: how we prepare our leaders to lead the fight (squad leader to 4-star general/admiral - professional development)
- **P**ersonnel: availability of qualified people for peacetime, wartime, and various operations
- **F**acilities: real property, installations, and industrial facilities (e.g. government-owned ammunition production facilities)
- **P**olicy: DoD/MoD, interagency, or international policy that impacts the other seven non-materiel elements.

Quite often additional two additional **I**-letters are attached to this acronym, emphasizing the missing (but relevant) elements – information and interoperability.

Capability can also be described as an effect or a function to execute tasks or as a fighting power through military units[11]. In principle, all warfighting is involved in solving the capability gaps between enemy’s and own troops’ capabilities.

This capability proportioned to the security environment prevents the emergence of crisis and their escalation to the use of armed force. Capability is assessed for Finland’s military defence and, at the same time, adapted to all tasks of the Defence Forces. The Defence Forces maintain the readiness level necessary to fulfil all tasks assigned to them. The use of the Defence Forces’ capabilities is prepared to cover the whole county.

2.3 Risk Environment

The comprehensive defence capability is not just limited to the capabilities owned by the FDF[12]. The preparedness of Finnish society is executed with the principle of comprehensive security, which entails the safeguarding of vital functions of society in a joint effort of the authorities, the business sector, organizations and citizens. The main reason for this national comprehensive defence system is a possible adversary – the enemy and its capabilities. This creates a threat. One way to analyze this threat is the risk management (see below).

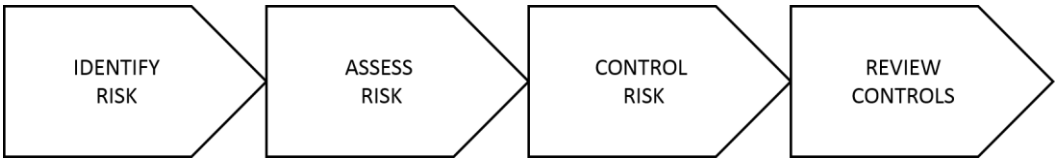

Figure 3: Principle of Risk Management

In risk management it is essential to identify possible risks, not only the current ones but also those, which can emerge in the future. Risks can be for example financial or political, but in the military context, risks occur often in dimensions.

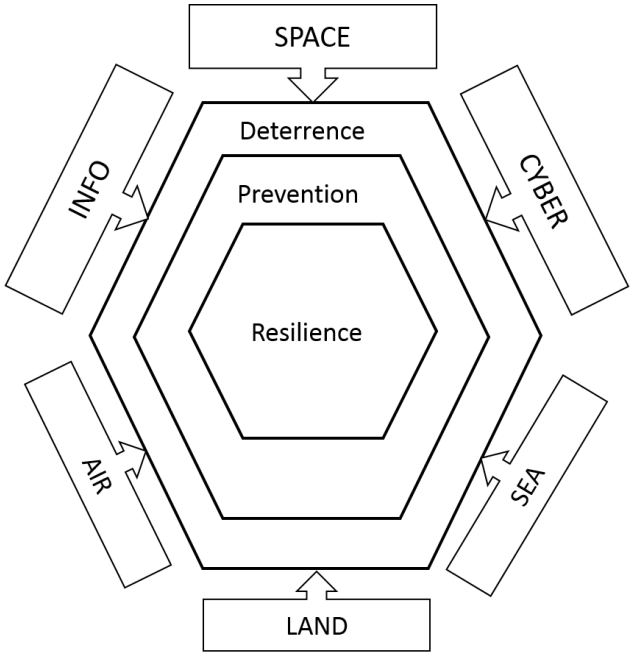

Figure 4: Defence layers and risk dimensions against external threats

The second phase is the risk assessment – how likely and how effective is the risk for the defence system. Without any deterrence, the threshold to use offensive activities drops. If the defensive activities fail (in the Prevention layer), the whole defence will depend on the resilience. Basically, the

whole defence is based on the questions: 1.) How prepared are You? 2.) How many offensive strikes You can block (simultaneously in the different dimensions) and 3.) How many strikes can You take without being knocked out?

The third part of risk management is trying to answer these questions. This work is constantly done under the first main process (capability plan and development). This also includes the strategic analysis to predict changes and new capability requirements for the future defence system. Sometimes predicted changes are disruptive and they launch a massive transformation for the whole defence system, but most of the changes are minor causing only small adjustments for the current system. On the fourth step of risk management, the need for reviewing controls is essential.

How is it possible to assess future changes? How many of these predicted changes are wide or even disruptive? What about timing, is there a need for immediate actions or is it possible to just wait and see? Should defence-planners abort their ongoing developments and acquisitions, if it is possible to predict that those subsystems will be obsolete the day they arrive to troops? What is the unbearable capability gap and are the decision-makers willing to take the risk connected to this gap? These tricky questions need to be solved. If it is possible to identify disruptive changes in the future and organization can make decision, are all the stakeholders prepared for a major transformation in the defence system if needed? The solution is not to rush into the future with high hopes according to the current trends of Artificial Intelligence, because that can lead to even a worse internal threat – building an uncontrollable system – "machine behavior"[13] without sense.

Rushing with the development can lead to unwanted consequences and waiting may lead to unbearable capability gaps. Something must be done, but with an overall understanding of consequences. Guidance of the development in system-of-systems-wide perspective requires an overall wisdom like approaching with the system thinking.

2.4 System thinking as an assurance of stable development

At present, Artificial Intelligence enables for example machines to make decisions, solve tasks and change their behavior according to circumstances, but is it possible to adopt military systems whose behavior is not fully known? Of course, it is possible with linear thinking - solving the facing problems one by one in a never-ending project. A more comprehensive solution is to rely on system thinking. The benefits of system thinking are described in the following table as an example.

Linear thinkers	System thinkers
Focused on the component or single subsystem	Concerned with the whole system of systems
Fixing the symptoms or coding errors	Trying to understand reasons and behaviour
Trying to control chaotic circumstances	Accepting the chaos but trying to find patterns
Believing that humans and organizations can be predicted, and they act always in logical order	Believing that humans and organizations cannot be predicted in chaotic environment
"Better blocks create better structures"	"Well-understood structure tolerates changes"

Table 1: Example of the differences in linear and system thinking

System thinking is also an essential prerequisite for the main research method, the soft system methodology, but before focusing on that, there is a need to investigate the other key factor in the changing future – Artificial Intelligence and its development.

On the next chapter, a brief look to the history of technology will reveal the origins of Artificial Intelligence and its possibilities to be a game changer. It is neither an official fact nor a fiction. It is a "what if" question and a possible challenge for the future defence systems. Does this lead to revolutionary or system-wide changes? Only the future can tell, but it would be wise to be prepared for unpleasant surprises too, or like Irish novelist Samuel Lover (1797-1868) wrote it - "better safe than sorry".

3 THE BURDEN OF HISTORY

To assess the Artificial Intelligence, it is always wise to take a glimpse to the history. The AI is just a consequence of the overall development of technology. Of course, it is impossible to fully predict the future according to the historical events, but it should be more like a broad-minded approach to the subject. We must also remember that "those who cannot remember the past are condemned to repeat it", ´like philosopher George Santayana (1863-1952) once said.

3.1 Brief history of technological development

The following figure presents a well-generalized description of the history of the technology.

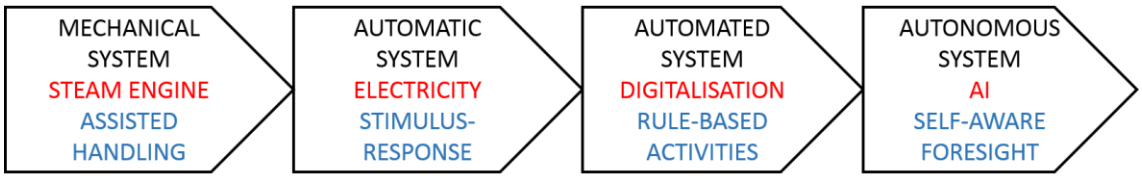

Figure 5: The history of technology - eras, enablers and typical features

Human beings have always been clever to invent new tools[14]. Through the history of humanity, tools have been used to ease daily tasks but also in warfighting. Certain inventions have been enablers to create new applications. New applications have changed the character of war, but only if there were necessary understanding of disruptiveness and will to change the system.

For example, the steam engine led to locomotives and steamships. Advanced mass transportation enabled less time-consuming ways to deploy forces to the operational area. There was no longer a need to guard all areas with fortresses, but only if the defence system was able to concentrate troops quickly enough. Of course, in that era, there were several other areas of development, like hydraulic systems, pneumatic systems and the combustion engine which enabled new war-fighting inventions like tanks and machine guns. Despite this, without common understanding, these new tools were used in the old way, which led to catastrophic losses of lives like in the World War I. New tools were ready, but the mind of the military leaders was obsolete[15].

The second great enabler was the invention of electricity. Electricity enabled numerous military applications like radios, radars, missiles, night vision gears, laser applications, etc. These tools were supposed to improve our capacity for independent action[16], but it also led to the first thoughts of automatic systems. In this era command, control and communication systems evolved very rapidly effecting especially to the OODA-loop. Time for observation, orientation, decision-making and action was dramatically shortened, and it appeared to be so, that human beings in this loop were considered to be the slowest part. First automatic systems started to do some human activities, but they

were not very sophisticated. Nevertheless, the role of human beings started to change, first slowly but then accelerating with something new - computers.

Computers launched the third era. With digitalization, the programmable machines were able to solve simple tasks. Through modeling and simulations, it became easier to make problem-solving algorithms. New kinds of capabilities and digitally improved old systems entered the battlefields. Sensor and data fusion enabled for example better battle management-, control- and targeting systems. Long-range-precision-weapon-systems enabled remote operations and the presence of human beings near the target was no more needed. As a matter of fact, the first questions about the necessity of human role in military operations were raised. Where do we need humans, which make military systems vulnerable, untrusted (old Latin saying: “errare humanum est”) and limited (reaction time, amount of memory, ability to calculate numerous possibilities and likelihoods of consequences of actions, etc.). Some western countries saw the problem as a legal or ethical question, while some other countries kept developing autonomous systems to achieve capabilities beyond human limitations forcing also the Finnish Defence Forces to react on the matter.

3.2 Challenges of automated systems

There is one enormous challenge to create fully functioning military systems with automated functions. The modern battlefield is a chaos and it is impossible to consider all the possible variables like deceptive actions, weather changes or enemy countermeasures.

All the possibilities need to be covered and even if that could be possible in the future (AI assisted programming), there is always a human factor involved – the human beings who create or accepts the code. Missing program code tends to cause unwanted activities or just nothing. A confused machine is an easy target for countermeasures. Similarly, too much confusing (dis-)information to handle leads to vulnerabilities.

Another major disadvantage of the automated systems is the lack of ability to learn in battle. Automated systems repeat the program time after time invariably and after a short follow-up, it is easy to predict the actions of automated systems and thus enable effective countermeasures.

The third major disadvantage of automated systems is the lack of situational awareness. Automated machines follow the pre-written rules and for example, breaking these rules to achieve better chances to gain higher-level objectives is not possible. On the other hand, it could be hazardous to create an algorithm with “the end justifies the means” – thinking. Of course, the history of mankind is full of this kind of thinking, like Arnaud Amalric stated: “Kill them all and let God sort them out”. The automated machines do not “know what is enough” and it doesn´t end it´s tasks until the preprogrammed conditions are fulfilled. This raises an essential question with a twist of fear - if you give the power to the machines, will it be lost forever?

The previous aspects emphasize the fourth disadvantage – how to trust "stupid" automated machines and how to ensure the man in the loop in all systems. The development of technology has enabled different kinds of semi-autonomous or assisting applications, like autopilot in airplanes but human beings have not been willing to give full control to the machines yet. No matter how simple activity is outsourced to a machine, human control is wanted. A typical example is the dead man´s switch[17] in locomotives – train is programmed to move on rails, but only if the driver press this switch regularly. Without pressing, the train stops. In this case, the minimum control is an availability to freeze the system if needed. This kind of back door is a little bit risky with the military systems and together with "better safe than sorry" security-oriented thinking, it has slowed down the deployment of robots and automated systems, especially in the western countries.

3.3 The next and the last level of technology – AI?

The next level of technology, Artificial Intelligence, could be a solution to these challenges but is the whole defence system ready for this wide change? Is there enough need, will and resources? How do the typical features of the defence system react to this change and how to make this happen? The main purpose of this study is not to create a full foresight picture of the future military AI applications or their consequences to the existing defence system. At this point, one major assumption is made – the AI is going to play a vital role in the future defence systems. Government wants it (excellence of AI application)[18], it offers multiple new possibilities and capabilities[19], other countries are on the way ahead[20] and the FDF is obligated to maintain develop defence capability in an operating environment that is in constant flux[21]. Hesitating will create capability gaps, but rushing can lead to very unpleasant consequences like Vernor Vinge stated: "But if technological singularity can happen, it will".

Evolving technology creates changes in the security environment, but how does it affect to the defence system? To understand that, a quick overview of typical features is provided in the next chapter.

4 TYPICAL FEATURES OF DEFENCE SYSTEM

Typical features of the system are effort and flow, information, energy and entropy[22]. The following picture describe them combined with the defence system.

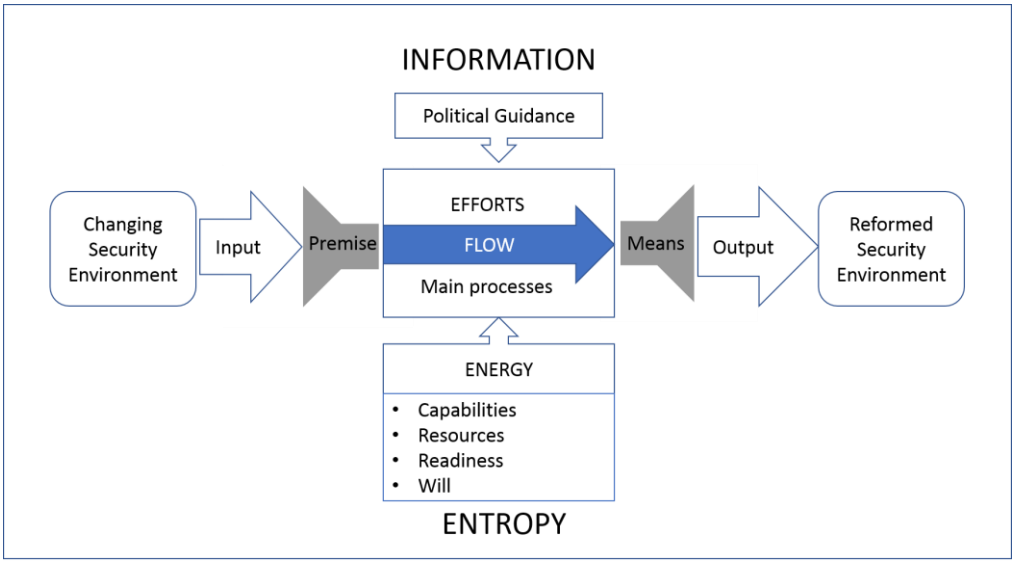

Figure 6: Systematic View of the Defence System

4.1 Efforts and the flow

The effort and flow of the defence system can be simplified to the main processes of the FDF. Processes combined with tasks and resources create the essence of whole system. All main processes are parallel, partly overlapping and consisting of several sub-processes. The input for the flow can be a product of the ongoing sub-process, like surveillance report of the enemy movements or it can be a given task, like a request to participate to peacekeeping operation abroad. All gathered inputs create premises of the flow, but the flow can affect with new input (gathering is parallel to the other ongoing processes) during the different phases of processes. Waiting, gathering and analyzing of this input takes time and delays the flow and one way to reinforce this flow is to freeze the premises to enable time-critical objectives. Sometimes quick implementation is better than a well-considered decision later in the hectic shifts of the dynamic environment.

The efforts are not limited to the FDF personnel. One of the key players is in the political guidance. Without proper legal legitimacy or an additional budget, it is impossible to utilize the full potential of the defence system. Similarly, there are many other external stakeholders whose capabilities are utilized but only if it is allowed. Urge to manage this net of stakeholders and capabilities has created new doctrines in some defence systems, like Network Centric Warfare[23].

All efforts are lost if the tasks cannot be fulfilled with the given resources in a certain time frame. It could be possible that the adversaries create new offensive capabilities with AI in the future and create an unbearable capability gap for the whole system. Deterrence can be created in traditional dimensions (land, sea and air at fig. 3) with non-AI-systems, but the other three dimensions could be more demanding in the future. In the hybrid warfare it is hard to make a difference between wartime hostile offensive activities and peacetime social disorder like AI-assisted targeting of fake news in social media. In the future, it could be more and more demanding to even decide are we at war or not (especially without own AI) and this hesitation will hamper the flow of the defence system. Activating defensive measures in the preventative layer will be late and the harm is done before effective countermeasures are even activated. So, the optimal flow is a sign of successful efforts and on the other hand successful efforts create an ongoing and meaningful flow to fulfil system´s purpose. In Maneuver Warfare[24] the target is the flow and that is achieved by negating the opponent's efforts - system collapses without great loss of energy and this energy can be reused afterward but of course in the hands of the winner. Maneuver Warfare has been a leading trend for the last 50 years but its "opponent" Attrition Warfare is raising especially in the nonlinear conflicts[25].

4.2 Energy

Energy means in this context all assets which enable efforts and flow. It has a strong connection to resources like time, money or personnel but in military context the capability is an overarching term connecting different elements together like earlier mentioned DOTMLPF-P.

Raising the defensive shields in different dimensions consumes time and other resources and it is essential to determine the response time (readiness) correctly. The most challenging response time is in the cyber and info dimensions, where hostile activities can be launched without pre-warning and with the speed of light in optical fibers. Preventing these kinds of offensive activities will be extremely hard in the future even with the AI-assisted defence systems. It seems to be so, that in the future, the nation and its citizens should tolerate more, and preventative activities and resilience should be notified even better in the future, like in the areas of education of media criticism and offline backup methods. It is especially important to remember that the defence system is as weak as its weakest dimension (and how that is handled). If the will of the people gets broken, efforts and the flow will fade. It is also essential to remember that the basic principle of the Attrition Warfare is to consume the opponent´s vital energy sources in order to collapse the system. But what is the vital energy source in the future battlefields? In the age of AI, could it be the information? Attrition of information could be impossible but what about the means to prevent the use of information – spoiling the information with credible disinformation? Contaminated information will eliminate the trust and without trust, there is no purpose for the system.

4.3 Information and entropy

In the defence systems, the information is present everywhere. More and more data has been digitalized and set available online. Information is taking a strong role in future battlefields, which can already be seen in concepts, like Information Warfare -concept[26]. This is not an entirely new thing on the battlefield and for example the Chinese general Sun Tzu's (510 BC) phrase "all warfare is based on deception" emphasizes the importance of information through the meaning of dis-information.

In the system view information means two things – it is a message and it is a reaction caused by that message[27]. If the information in the input is wrong and it passes the analysis, the whole flow is meaningless causing unwanted outputs. Of course, the information may turn out to disinformation in every phase of processes, especially when the human interaction is involved. To prevent this, every process phase may include fact checking activities, but this might delay the flow too much, because the timeliness is also essential element of the information. One way to describe the flow of information is shown in the picture below, based on the Claude Shannon's diagram of a general communications system.

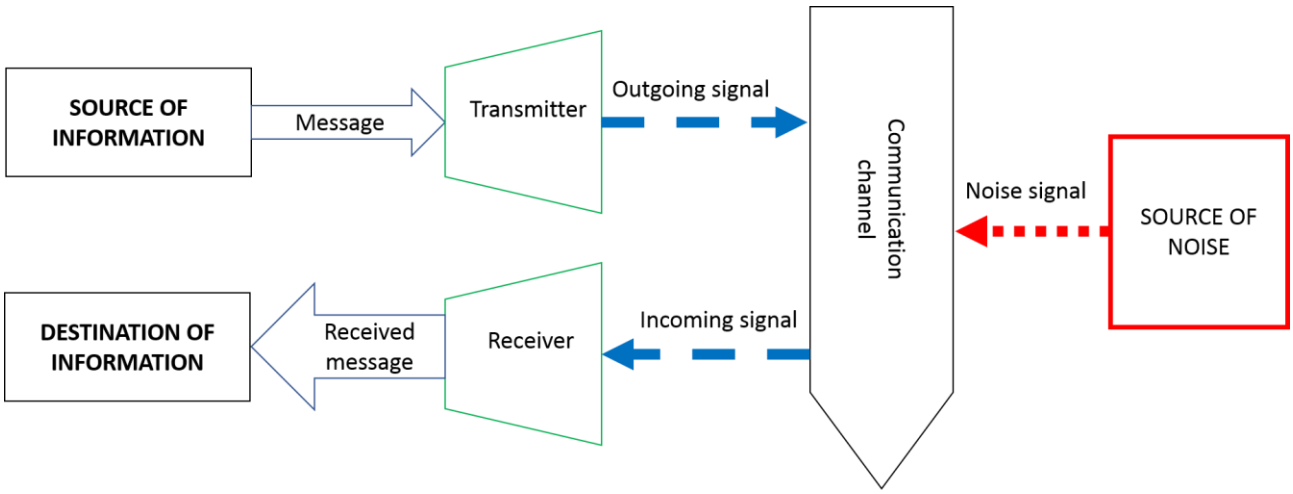

Figure 7: General communications system

Obsolete information becomes unusable in the hectic changes of chaos like the events of modern and future battlefields. There are various ways to assess Information Quality (later IQ) and here is one example – a typical list of IQ elements[28]:

1.) Intrinsic IQ: accuracy, objectivity, believability, reputation
2.) Contextual IQ: relevance, value-added, timeliness, completeness, amount of information
3.) Representational IQ: interpretability, format, coherence, compatibility
4.) Accessibility IQ: accessibility, access security

What is the meaning of the received information and how is that connected to the term entropy? The basic idea of the information theory is that the "news value" of a communicated message depends on the degree to which the content of the message is surprising. More surprising means more entropy. More and more data mean more information, disinformation and entropy. Military operations are based on the planning - producing preparations and plans. Enough entropy has an effect to crush those plans, but what happens if the AI will take care of the planning. Full modeling of the battlefield and simulated flow of all possible events may create an unbeatable master plan. This AI-enabled master plan would be a constantly updating database providing all the possible plans and preparations for the present and future. Without surprise, there is no room for entropy. Without deception, is there room for Maneuver Warfare? Is this a path to the next worldwide war with means of Attrition Warfare and total destruction? If AI can foresee this (all possible scenarios are in the master plan), would it allow it? Maybe planning machines can “understand” this end state without singularity and the singularity will just be the final activity to gain control of the defence system to prevent full-scale destruction. This doesn´t necessarily mean the future, where self-aware killer robots are hunting down the last remains of humans. The solution could be simpler – AI will just switch off the essential systems. The total blackout of communications will do the trick.

How is it possible to develop a future defence system and bear in mind all the possible consequences of AI in the different steps? The next chapter will approach this with the Soft System Methodology.

5 APPROACH WITH THE SOFT SYSTEM METHODOLOGY

Systems thinking is a holistic approach to focus on questions like how the system's constituent parts interrelate and interact within the context of larger systems and how the systems work as time passes. System thinking is an overarching term for the developed collection of methods – system methodology[29]. This methodology is suitable for the future studies, when the area of study is complex, organized, self-regulating, dynamic and in interaction with its environment. Soft System Methodology (later SSM) created by Peter Checkland and his colleagues has been developed to understand complex problems and processes and to manage the major changes in systems[30]. Based on this, SSM has been chosen in this research to solve the main question – how the Finnish Defence Forces can in the future implement applications of Artificial Intelligence to the defence system without unwanted consequences.

The SSM can be divided into seven steps, which are described in the following picture.

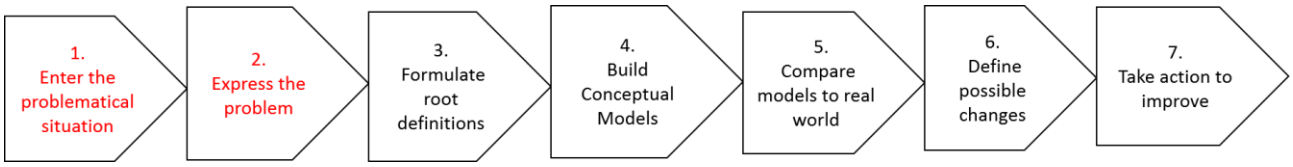

Figure 8: seven steps of Soft System Methodology

This study will cover the first six steps, emphasizing the red-colored ones in picture 8. The first step is discussed in the previous chapters, this chapter is focused on the problem and the following chapters cover the steps 3 to 6. The last one is left to the decision-makers if they decide to utilize the results of this study.

5.1 Expressing the problem

Implementing the AI to the defence system, how hard can that be? This question is relevant, and it seems to be easy to answer if the details are not concerned. But as in matter of fact "the Devil is in the details, but so is the salvation" by Hyman G. Rickover (1900-1986)[31] is one way of expressing why this problem is so complex. As soon as different stakeholders start to discuss the matter from their own point of view, the divergence will emerge. Different interests, opinions and expectations of stakeholders will create multiple new requirements, desires and service needs. Simultaneously the accelerating development of AI applications will create pressure on the decision-makers, and all the time more and more of the sub-systems seem to become obsolete creating demands for life-cycle updates and new acquisitions to avoid unbearable capability gaps. On the next table, there is a hypothetical list of stakeholders and "a wish list" of future AI applications.

Stakeholder	Future AI application	Purpose / Example / Notice
Army	Battle management system	Assisted decision making [32]
Navy	Loitering weapon system	"Self-aware" sea mine [33]
Air Force	Unmanned combat aerial vehicle (UCAV)	Man-machine teaming [34]
J2 (Intelligence)	Synthetic aperture radar satellite constellation	Swarming, data fusion[35]
J4 (Logistic)	AI assisted Enterprise Resource Planning	SAP Conversational AI [36]
J6 (C4)	Cyber security countermeasures with AI	Cyber-attack defence [37]

Table 2: Example of the future AI applications

Table 2 is just a hypothetical example, but it describes how the goals may differ within the organization. Artificial Intelligence can emerge in various ways, but what is the real value of a certain AI application to the whole system? Some applications have overlapping activities, and some are prerequisites for others. Is this complexity too difficult to solve without General Artificial Intelligence? Waiting for that is not an option.

System thinking prefers focusing on the processes. Would it be clever to concentrate on the main processes? It might be easier to make framework solutions on the higher level, formulate a vision with milestones and after that it could be time to solve details. Nevertheless, a simplified approach to AI applications is still needed and one way to do this is to use categorizing.

There are several ways to categorize AI applications in defence system and for example one recent list consists of military drones for surveillance, robot soldiers for combat, intelligent systems for awareness and secure web-portals for cybersecurity[38]. List is good for the present situation, but it is a little bit too narrow for more open-minded thoughts of the future. In this study the AI-applications are divided into four categories to clarify the review. These categories are:

- AI-assisted decision-making (including situational awareness)
- Autonomous systems (full or partly autonomous)
- AI-assisted management in cyber-warfare
- AI-improved legacy capabilities (including man-machine teaming)

In the following table previously mentioned main processes and categories are combined to identify possible risks - too slow progress and on the other hand too urgent implementation of AI applications.

MAIN PROCESS	CATEGORY	RISK IN TOO SLOW PROGRESS	RISK IN TOO FAST PROGRESS
Capability plan and development	Decision-making	Capability gap in reaction time	Distrust in the system
Capability plan and development	Autonomous systems	Capability caps in management	Inadequate modeling and simulation
Capability building and maintenance	Cyber warfare	Obsolete versions of programs	Too dependent to foreign corporations
Capability building and maintenance	Improved capabilities	Obsolete systems on arrival	Problems in configuration management
Capability building and maintenance	Autonomous systems	Obsolete systems on arrival	Poor technical readiness
Readiness control and use of capabilities	Decision-making	Distractible with updated AI versions	Legal and ethical problems
Readiness control and use of capabilities	Autonomous systems	Capability gaps in countermeasures	Symptoms of singularity
Readiness control and use of capabilities	Cyber warfare	Too slow reaction time	Unintended collateral damages
Service activities	Decision making	Cost-efficiency problems with parallel systems	Too dependent to foreign corporations
Service activities	Improved capabilities	Interoperability problems	Man-machine-teaming problems

Table 3: Example of possible risks

Even on the level of main processes, there seems to be plenty of unsolved problems for the future. The use of AI in military applications is increasing and the plans to cover even more challenging or wider areas like strategic decision-making, education, training or executing military operations have been discussed[39]. This requires hard work like research, analysis, interactivity within and between stakeholders and decision-making. The common understanding of the problem, goal setting and mutual commitment in the organization is essential, before proceeding to the next step - defining the solutions for existing problems.

5.2 Toward to the next steps

When the problem is clear, the next step is to define a common vision. It guides the change towards the right destination and to change the system, a model is needed to manage this. One example of the model is the Kotter´s 8-step Change model[40], which is presented here. The basic principle is described below.

Figure 9: Kotter´s 8-step change model

The Soft System Methodology has some similar features to Kotter´s model. The main difference is an element that is missing in the Kotter´s model – it is the understanding of where we are now. In Kotter's model the difference of the current state and vision is clear, but that is not necessarily always so with complex systems and human interactions. So, the vital question is, where are we now with this Artificial Intelligence revolution?[41] Is it going to become reality soon or are we facing just another AI winter, caused by failed expectations? What is different from today's AI research compared to the former drawbacks? If the present defines the future, is the state of current development an avoidable subject to study?

Before moving on to the next steps in the soft system methodology, the following chapter provides a concise description of the current state of AI.

6 CURRENT STATE OF AI

Today Artificial Intelligence refers to an artificial creation of human-like intelligence that can learn, reason, plan, perceive, or process natural language. There is a possibility to discuss this matter very thoroughly, approach it with different methods and raise questions like what does the artificial or intelligence mean from the philosophical or technological point of view. The scope of this study is limited, so it is concentrating to Artificial Intelligence as a wide and evolving research field, but it is important to understand that AI is not some trendy subject reserved for experts to talk about or dream that might come true in the distant future. The products from the earlier AI research are already activated and we are using them knowingly or unknowingly. The Artificial Intelligence is not coming – it is already here.

This chapter includes the current uses of AI, the most important research areas, and ideas of the future possibilities. This will reveal the present existence of the AI, but also the challenges of today's work. AI has also the potential to change the way that humans interact, not only with the digital world, but also with each other, through their work and other socio-economic institutions[42]. This study has limited scope and covering all aspects, consequences and meanings is not possible, but a common understanding of the present state – where are we standing now, is important before taking further steps toward the future.

6.1 Current use and research of AI

The fruits of the AI development enable exploiting of them in the different areas, but this possibility does not mean that it is easy to execute[43]. Despite the promising research results of the novel AI concepts, the road for a successful implementation or a full operational capability in military terms is quite often a demanding and time-consuming process. The main bottlenecks holding back further adoption of AI has been studied earlier and findings reveal that following reasons are the most common ones: the need for AI is not recognized, the lack of adequate data, the lack of skilled people, difficulties to identify business opportunities, challenges with technological infrastructure and legal concerns[44]. Despite these challenges, the problems have been solved in several areas and it is easy to show that the huge impact of AI development for our every-day life is clear. The AI is already used intensively for example in the following fields: virtual assistant including chatbots, agriculture and farming, autonomous flying, trading, security, surveillance, sports, manufacturing, inventory, self-driving cars, healthcare, and warehousing[45].

The current use of AI is spread over a wide area, but does it affect only a few people? The following table gathers some essential examples to estimate the number of users.

Implementation	AI research area	Estimation of users
Apple: Siri - voice assistant	Speech recognition	500 000 000 [46]
Netflix: personalization	Recommender systems	167 000 000 [47]
Facebook: bad content detecting	Deep learning	800 000 000 [48]
Google: RankBrain - querie optimization	Machine learning	1700 000 000 [49]
Owners of the smartphones	all above and more	3500 000 000 [50]

Table 4: Proof of AI users worldwide

Today's most popular AI research areas are Machine Learning, Deep Learning, Natural Language Processing, Recommender Systems, Robotics, Computer Vision, and Internet of Things. Every one of these is a large research area making it impossible to cover them thoroughly in the scope of this study. The following table provides a short example of the main features of the four research areas.

Main area	General types	Essential feature
Machine Learning	Supervised learning	The learning algorithm is given labeled data and the desired output and so the algorithm is helped to learn
	Unsupervised learning	The data is unlabeled, and the algorithm is asked to identify patterns in the input data. Finding similarities is a key for learning
	Reinforcement learning	The algorithm interacts with the environment that provides positive or negative feedback. Learning by doing is essential.
Deep Learning	Unsupervised Pre-trained Networks	Train the neural network with unlabeled data, do modifications and train again, now with the labeled data.
	Convolutional Neural Networks	Input is typically an image, which is filtered with the independent convolutional layers. Pooling layers are used to reduce size.
	Recurrent Neural Networks	Network where the output from the previous layer is fed as input to the current layer.
	Recursive Neural Networks	Repeating the data flow several times and comparing each round the result to the expected value and using this error for the adjustments for the next round until the error is minimized.
Natural Language Processing	Syntactic analysis	The arrangement of words in a sentence is on the focus of creating an algorithm so that makes grammatical sense.
	Semantic analysis	Applying computer algorithms to understand the meaning and interpretation of words and how sentences are structured.
Recommender Systems	Content-based	Based on the information about the specific case, who did and what exactly was done?
	Collaborative filtering	Based on the background information, what kind of people do similar things and behave in the same way?
	Hybrid systems	Combines Content-based and Collaborative filtering.

Table 5: Example of typical features in four areas of AI research

Some of these areas of research intent to solve complex problems alone and some tend to join with others or new technology fields, like quantum computing. The speed of development is increasing and the capability to solve all the time more and more complex problem is getting better. Multidimensional data sets some barriers through limited computing capability but hopes for the future are extremely high. But disappointments have happened and will happen in the future. The key question is, how to pinpoint the surest and on the other hand most impressive research projects for the future?

6.2 Foreseeing the future of AI

There are several ways to get lost in predicting the future of AI, but for example the MIT Technology Review's list "The Seven Deadly Sins of AI Predictions" from 2017 is still a valid guide to keep on track[51]. Overestimating, underestimating, imagining magic and Hollywood scenarios influence the decision-makers, and the externally generated internal pressure to follow trends create a sense of urgency. Starting points are not favorable for making sensible decisions. The easiest solution is to just follow what others are doing, but that is not a completely risk-free option either. Some of the presented new intents may be purposive and guide further research to certain areas to create a common interest, economic benefit, or a monopoly position elsewhere. A sense of urgency and the mixture of dis-information and information hampers the future foresight of AI, uncertainty arises and causes a crisis with strong emotions like panic, paralysis, or grief. The relevance of this type of grief is weak to the Kübler-Ross Grief Cycle model, but peculiarly, the first stage of denial rings a bell – ignorance of the Artificial Intelligence often leads to denying to its existence or meaning for the future. The only way to fight against this ignorance is to increase the amount of knowledge in the organization.

To maintain credibility in the organization, the shared information should be based on facts, but the nature of the future does not allow this. The future is loaded with some uncertainty and the amount of it seems to be increasing. The only certainty for the future might be the uncertainty[52], but is this just a mark that the warfighting in the info-dimension has reached its goals? To prevent that not to happen, the pursuit for achieving more information about future must continue.

Another challenging feature in the future foreseeing is the self-fulfilling prophecy in the causal loop. Fulfilling the prophecies of the provided hype loops or future trend lists can lead to an influence of behavior which confirms the relevance of adopted prophecy. To maintain objectivity and relevance over time in this report any of the present existing hype loops, trend lists, or any other form of prophecy is not presented here. Instead of that, the following table is created to show what kinds of means are available for monitoring the future development of AI.

Means	Explanation
Future studies	A scientific approach includes various of methods, e.g. Popper's diamond[53].
Web scanning	Systems or services to seek information about new research projects.
IPR scanning	Systems or services to seek information about new copyrights, patents, designs and trademarks and all other changes of intellectual properties rights.
Target mapping	Seeking for complex problems that could be solved with the future AI inventions, e.g. improving the understanding of genomic libraries, interaction between features in the battlefield or instant data fusion of hyperspectral sensors.
Investment research	Following the funding of AI-related investments and identifying the key players.

Table 6: Example of means for monitoring the future

The research area of AI is wide and all the time expanding. This problem cannot be solved separately by concentrating on one research area or fixing one subsystem at a time, which emphasizes that a decent approach with a system thinking is needed. The main questions of this study remain - how to prepare the Finnish Defence System for the future development of Artificial Intelligence. Is it possible to combine the development of AI and the development of the military capabilities in the Finnish Defence Forces? In the next chapter the synthesis is approached with the next steps of the Soft System Methodology, covering steps from 3 to 5.

7 SEEKING FOR THE SOLUTION

In this chapter the previously described problem is approached with further steps of the Soft System Methodology. A root definition can be considered as a structured description of a system[54] while deriving a conceptual model is more like a method of analyzing the activities which need to take place in to clearly define what the actors need to do in order to achieve the transformation[55]. The last section of this chapter includes a preliminary assessment between the presented models.

7.1 Root definitions

Approaching towards previously presented vision - "In the year 2040 functions at all the different levels of the Finnish Defense System are supported by artificial intelligence applications including support to the decision-making and controlled use of autonomous systems" needs to be clarified. This is done by root definitions that split up the problem into smaller areas of human activities which reflect separate goals. This splitting should be done according to the governmental guidance. In Finland, there is no such overall guide like the United Kingdom has online – "A guide to using artificial intelligence in the public sector"[56]. This is utilized in benchmarking later in this study, but the following key areas are based on the Publications of the Finnish Ministry of Economic Affairs and Employment, " Leading the way into the age of artificial intelligence - Final report of Finland's Artificial Intelligence Programme 2019 Publications ". According to the statement from the Ministry of Defence on the 31st of October in 2018, the guidelines in this report should be highlighted even more prominently and, if possible, condensed and concretized[57]. The following table of root definitions is determined according to this statement with the CATWOE framework presented in the appendix.

Key actions (" Leading the way into the age of artificial intelligence" -report)	Refined root definitions (activities in the Finnish Defence Forces main processes)
1. Enhance business competitiveness using AI	RD_1: Planning and development personnel should identify and focus on the utilization of artificial intelligence in the development of military capabilities
2. Effectively utilize data in all sectors	RD_2: All personnel should identify existing data in the daily activities, create or improve means to collect it and share the information of the gathered data.
3. Ensure that AI can be adopted more quickly and easily	RD_3: Capability building personnel should ensure that the required level of education in AI is achieved and updated to all personnel

4. Ensure top-level expertise and attract top experts	RD_4: Planning and development personnel should re-evaluate recruiting strategy and create AI positive organization culture.
5. Make bold decisions and investments	RD_5: Planning and development personnel should approve a certain level of uncertainty and make necessary commitments for agile activities with AI.
6. Build the world's best public services	RD_6: Personnel in service activities should reflect the AI excellence of the organization with state-of-the-art service systems.
7. Establish new models for collaboration	RD_7: Planning and development personnel should establish new AI-oriented platforms and means to enhance collaboration with various of stakeholders
8. Make Finland a forerunner in the age of artificial intelligence	RD_8: Planning and development personnel should invest in AI-related research and innovation which support the development of military capabilities.
9. Prepare for artificial intelligence to change the nature of work	RD_9: Personnel of readiness control and use of capabilities should monitor the environment for any signs and effects of use of Artificial Intelligence.
10. Steer AI development into a trust-based, human-centric direction	RD_10: All personnel should be aware of the instructions and restrictions and follow them.
11. Prepare for security challenges	RD_11: Planning and development personnel should fortify the defence of the cyber and info dimension.

Table 7: Root definitions

These root definitions are used as building blocks for creating models. To simplify visualization the following numbering with defined keywords are used in further work:

RD_1 MONITOR meaning root definition 1 – Create situational awareness
RD_2 COLLECT meaning root definition 2 – Collection of data
RD_3 EDUCATE meaning root definition 3 – Education and training of personnel
RD_4 MOTIVATE meaning root definition 4 – Win the hearts and minds of personnel
RD_5 AGILITY meaning root definition 5 – Create basis for agile development
RD_6 SHOW meaning root definition 6 – Reflect the skills of organization
RD_7 CRADLE meaning root definition 7 – Create experimental platforms
RD_8 PROJECT meaning root definition 8 – Invest to the new projects
RD_9 LEARN meaning root definition 9 – Research causality
RD_10 LEGAL meaning root definition 10 – Solve the legal questions
RD_11 PROTECT meaning root definition 11 – Protect Data

7.2 Building conceptual models

A conceptual model is a representation of a system. In this case, it represents the arrangements of building blocks based on root definitions. It is possible to arrange building blocks on the future timeline in several ways, but some restrictions should be notified. The first one is the interaction of building blocks, because the order and combination of the blocks determine the overall effects of the whole system. For example, it is possible to create AI-application without planning and related documentation, but the problems start when approval for production or use is claimed. The following figure reveals some of the most obvious interactions, simplified by single verbs.

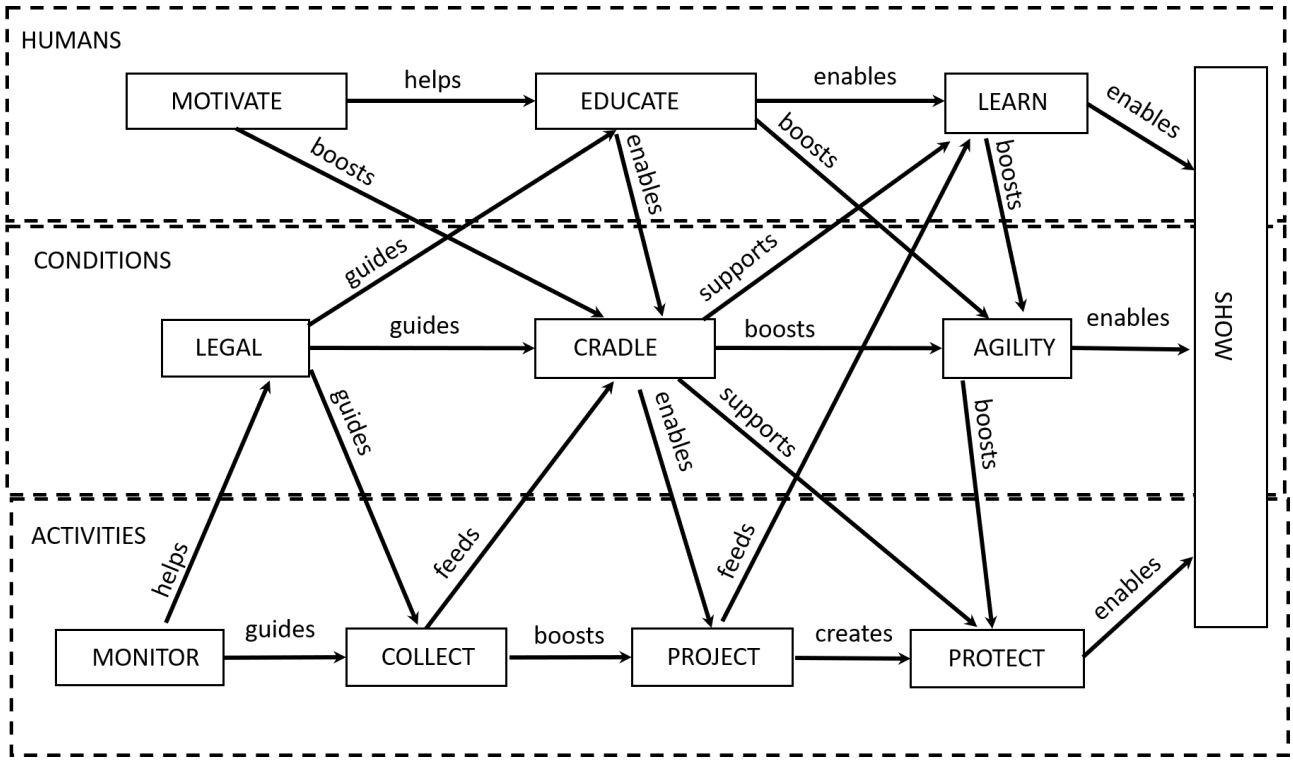

Figure 10: Some interactions of building blocks

The second determining factor is the project management triangle[58], meaning that the time, cost and quality have a dependency on each other. Meeting high expectations in a short period of time requires a lot of resources and finding quick profits with limited resources degrades quality.

The third factor is the risk management[59], emphasizing the identification and assessment of possible risks. All these factors interact with each other and a thorough analysis would require a broader and more comprehensive research. The following four models are created with the basic principles of these factors and deductive reasoning.

7.2.1 Turtle model

Turtle model is based on avoiding risks and practicing cautious development - starting with monitoring to direct further activities without risks. Legal aspects strongly guide the development from the very beginning and first platforms are based only after the major legal questions are solved. Learning is basically about detecting mistakes and success stories done by others. Collection of data begins after the rules and platforms are fully developed and protection of gathered data is guaranteed. Agility is treated as add-on and special case in defined projects, which are launched after the personnel is trained for that. The achievements are presented as a result of hard work.

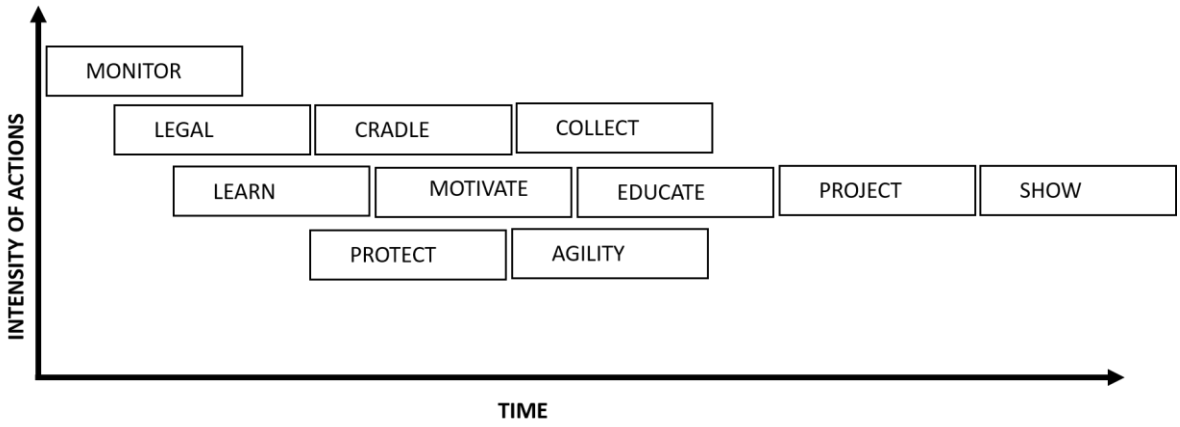

Figure 11: Turtle model

Turtle model has its advantages and disadvantages. Development avoids risks but it takes a long time. Actions are evenly distributed, meaning that the resource demand has no significant peaks.

7.2.2 Pathfinder model

The Pathfinder model is based on taking risks with agile development to achieve a leading position. Development is front-loaded emphasizing quick start with data collection, increasement of agility and establishment of new platforms. Monitoring is focused on the new inventions and possibilities for the national co-operation. New AI-oriented experts will be hired, and information campaigns are launched to manage resistance to change. The goal is to quickly launch fore-runner projects and utilize gained experience in personnel training that takes place parallelly. Working with novel projects reflects the excellence of the organization. Learning from own development reveals new possibilities and countermeasures to protect gained data. Arising legal questions are solved ad hoc or postponed to the future.

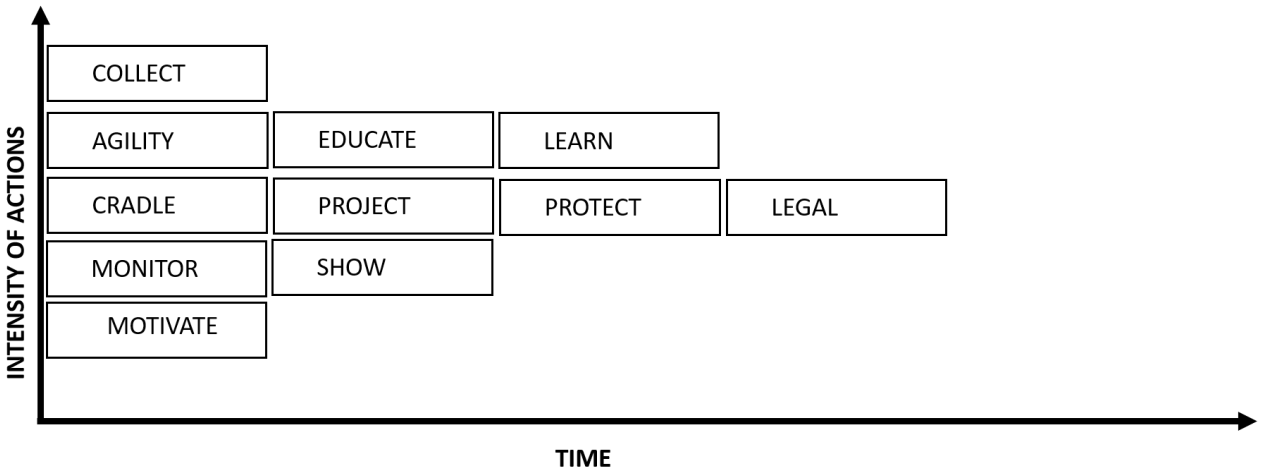

Figure 12: Pathfinder model

The Pathfinder model requires plenty of resources at the beginning, but it creates results in the relatively short period. Known risks are accepted but some unexpected ones will also occur.

7.2.3 Mule model

The Mule model is based on carrying the whole load of development alone. It combines the Pathfinder´s agile thinking and Turtle´s cautious development. The load of the risk management and pursuit of agility is bearable when building blocks are distributed more evenly over time. It allows more parallel operations and thus limits the time required. It starts with legal issues, but allows earlier starting of other blocks, when identified and solved key questions are solved. Monitoring guides the collection of data to the essential fields of AI. Protection and arrangements to store and utilize data are in the vital roles from the beginning. Personnel will be motivated and encouraged to data collection simultaneously with necessary process changes to increase agility.

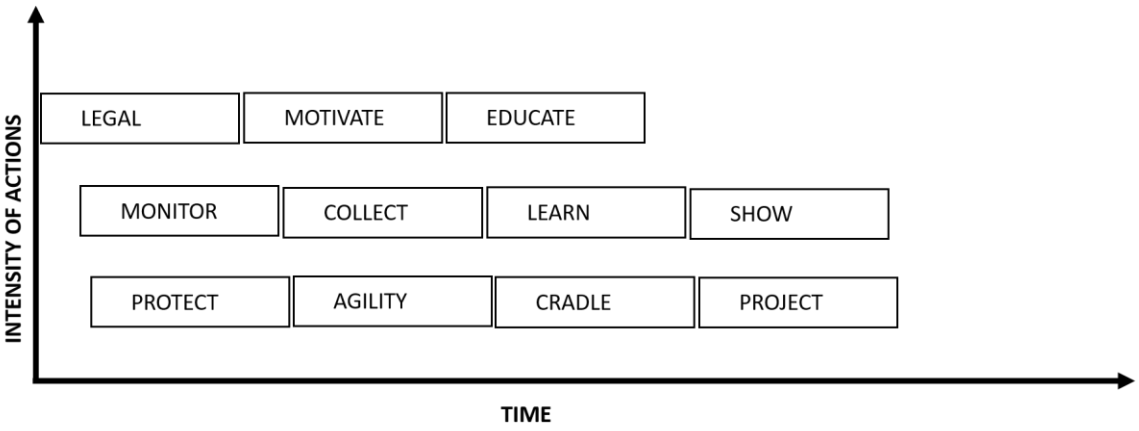

Figure 13: Mule model

The Mule model counts on the efforts of humans in organization, because many blocks activate simultaneously, and old processes are transformed on the run. Platforms are created ad hoc to launch agile projects and capability for that is presented as a result of successful transformation.
This model also combines the negative sides of previously presented models. It requires resources and commitments that will last throughout the change but will eventually achieve an agile nature.

7.2.4 Ants model

The Ants model is based on broad collaboration and concentrating nationally on specific areas. Parallel activities are enabled through national and international co-operation and divided responsibilities between stakeholders. The legal perspective focuses on reaching consensus and binding agreements. Benchmarking will be a continuous process of comparing own processes and performance metrics to the best practices from other partners. Pooling and sharing assets between partners speed up the change, but for example, the cultural differences acquire additional work. Open access to all AI-programs led by partners builds trust and competence of participating stakeholders. The lessons learned process boosts the development and prevents failures from being repeated. Parts of the protection will be outsourced but the overall protection in cyber and info dimensions increases through decentralizing of assets and existence of joint capabilities. Showing own state of the art in certain AI-areas guarantees the membership in the development alliance.

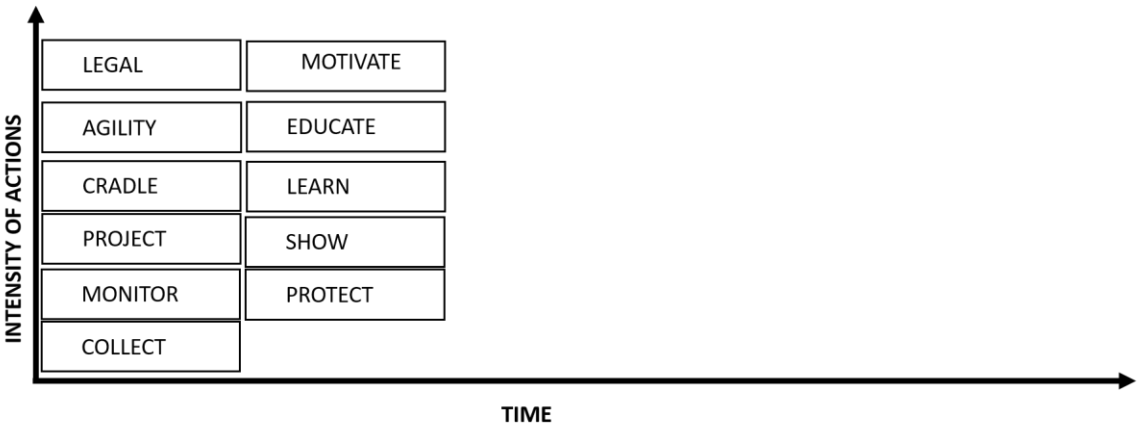

Figure 14: Ants model

The biggest disadvantage of the Ants model is the dependence on national and international partners. Commitment for the long-term co-operation creates new requirements and needs for standardization to ensure full interoperability between partners. The estimation of this cost needs further research.

7.3 Models and the real world

This section includes a preliminary assessment of the previously presented models. It is based on the risks identified during this research and the risks which are based on the lack of prerequisites for AI-development work. This assessment without scaling and weights offers just one simplified example of how to implement an assessment between different models. The influence of differently weighted risks significantly affects the results. On the other hand, deliberate shifting of weights allows achieving the desired results, highlighting the importance of consensus among stakeholders in prioritizing different risks. A more comprehensive research is needed to define justified weights on different risks, which is limited beyond this study, but the value of understanding the risks associated with the future work of Artificial Intelligence in the defense context remains valid.

7.3.1 Identified risks of the system

There are several benefits and risks of Artificial Intelligence and several myths about advanced AI has been presented in public[60]. In this section the risks are identified from the systematic view on the previously presented system. Several individually identified risks have been grouped into five risk entities to streamline processing. They are presented below in no particular order.

The first one is the risk of a capability gap. The gap arises for several reasons, but the most important of these is the obsolescence of existing systems. The development of capabilities in one or more defense dimensions is not enough, and the performance of countermeasures or resilience is not updated to match the emerging threat. The aim of superior military technology with AI may lead to a new era of arms race meaning competing with the latest updates to gain superiority through the more sophisticated autonomous systems than the opponent has. Allowing some gap is economically wise but the thin line between “good enough” and unbearable risk is getting narrower in the future. The concept of exploiting the weaknesses of stupid systems as a method of waging a war will be an advantage for the leading AI actors. As "soft targets", the control mechanisms of AI systems will be targeted first.

The second risk is the loss of control which refers to an inability to control the development of the system, the system itself or the ability to anticipate its behavior. The worst fear is the singularity but there are also more common ways to lose control, like a fatal error in programming, hijacking or an unexpected end of support from a strategic partner. It is pointless to use resources to deploy systems that cannot be controlled.

The third risk is the waste of effort, which means that little or no results with AI are achieved compared to the spent resources. This has a strong connection to the previous ones, but the manage-

ment of this risk emphasizes the ability to guide the development process in order to gain cost-effectiveness. The valued resources—time, money, labor, tools, infrastructure, and raw materials, including data, should all be used in a meaningful way. If not, the trust starts to deteriorate.

The fourth risk is a loss of trust. The philosophical relation between trust and risk is a special topic and for example the Handbook of Risk Theory deals with that subject in depth[61], and in this case trust is reflected through responsibilities of trusted AI-systems to fulfill. Unexpected machine behavior, conflicts with man-machine-teaming and unintentional machine learning of "bad habits" are obvious reasons for distrust. A more challenging subject is the humans' blind trust in the black boxes, meaning, for example, human's limited ability for understanding multidimensional data in deep neural networks. "If it works, why bother exploring its functionality" -thinking may take the whole humankind to the path with no return.

The last entity is the risk of violations against national commitments. According to the Europeans commissions ethics guidelines, trustworthy AI should be lawful, ethical and robust[62]. Development of AI-related systems should follow the international commitments and national legislation, but the increasing speed of technological development in AI makes it controversial. It is always possible that ex-post legislation will invalidate the results of the development thus causing a waste of resources. There are several other relations between presented risk entities, but their interdependencies are beyond the scope of this study.

7.3.2 Missing performance considered as a risk

Agile software development is not an entirely new subject, meaning that the principles, patterns and practices have been under research from the beginning of the 21st century[63]. The implementation of the "agile means" differs between AI-projects and different guides are presented on the subject[64], but the principles of the needed performance can be described through the concept of capability. The following picture encapsulates the essential aspects of AI capability for agile software projects.

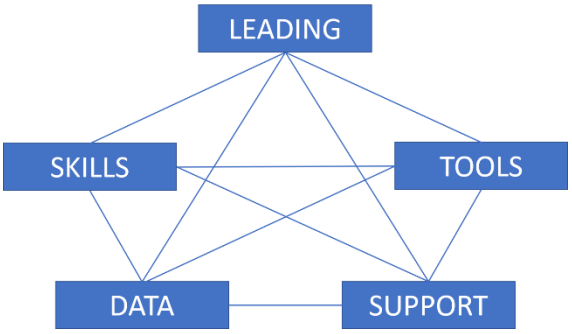

Figure 15: Capability aspects of AI development

The leading aspect includes the management and leadership of the decision-makers. Setting clear expectations, acquiring adequate subject and project understanding and team-leading skills can be the vital prerequisites for a successful project[65]. Clear responsibilities, solid commitments, motivating activities and building the AI-supportive organizational culture are also important. Lack of any mentioned subjects or controversial activity is considered as a risk in the following analysis.

The second aspect, skills, refers to the quality and quantity of personnel involved in the AI project. A "dream team" of AI project can, for example, consist of machine learning engineers, data integration engineers, software developers, user experience designers and Agile coaches[66]. The agile method, like pair programming, doubles the amount of participating people, but the benefits for the whole project can be huge[67]. Gathering identified experts is important, but just as important is keeping them throughout the project. Avoiding the "brain leaks" may become the hardest challenge of the organizations for the next years. Timely insufficient knowledge is defined in this context as a risk.

The third aspect is the existence of an accessible and up-to-date set of tools needed in development work. Data preprocessing, orchestration, source control, collaboration, debugging, and testing are examples of areas where effective tools make the difference. Sometimes the development of tools is a prerequisite for proceeding in the projects and on the other hand obsolete tools can paralyze the whole progress. Insufficient investing in software and hardware at the right time is an obvious risk.

The fourth aspect refers to the quality and quantity of data. Data can be considered as raw material of information[68], but also the importance of labeled data, for example, in machine learning is vital. Enough high-quality data ensures better results while an insufficient amount of low-quality data can prevent the desired learning[69]. Problems related to the quantity, quality or timeliness of the data are considered as a risk in this case.

The fifth aspect refers to infrastructure and services which enable development work. Infrastructure can mean a physical structure, such as a laboratory building for a secure test environment or a safe test field for autonomous systems. Services like outsourced data storage, network security and future quantum computing may have an increasing role in the future when the multidimensional Big Data is fully utilized.

7.4 Comparison of the models by deductive reasoning

The following evaluation of the four conceptual models is performed by deductive reasoning. Probability differences are not scaled, and sequence numbering is used instead. This ordinal scale is a measurement that indicates the ranking and ordering of the models without establishing the degree of variation between them. As a risk score, the higher numbers mean more risk**.**

The first system risk refers to ending up into the capability gap. The speed and scope of development activities are essential in the assessment. The Turtle model with slow progress and limited scope represents the highest risk score with number 4. The Ants model enables rapid development over a wide area with multiple assets and the lowest risk score - 1 is thus justified. The Pathfinder model with risk score 2 is more agile than the Mule model with the risk score 3.

The second system risk refers to the aspect of losing control. Several factors affect the assessment, but the level of knowledge and circumstances (tools, platforms and services) are highly valued. The turtle model has the lowest score with cautious proceeding. The Ants model offers expertise and circumstances, thus deserving the second place. The Pathfinder model with early investments to the circumstances, end up to the third place compared to the Mule model ending up to the least score.

The third system risk refers to the risk of unproductive investment. The intensity and scope of investments are important in the assessment, but also the means of sharing risk areas and the overall control of the development are considered. The Pathfinder model with built-in risk-taking, both intensity and scope, means the highest risk score. The Turtle model produces the second-highest risk score because the possibility to implement obsolete products is extremely high. Investments in the multinational collaboration enables sharing the risks but the joint control may become challenging according to the lessons learned[70]. This means that the Mule model ends up with the lowest risk score despite its challenges in controlling the parallel activities.

On the fourth system risk, the risk of losing trust is in focus. Assessment of the trust is based on the activities affecting human knowledge, motivation and experiences with AI-related systems. This has a strong relation to the previously presented second risk – losing control, but this risk is focused on human minds rather than technical issues. With the Turtle model, working with AI is distant for most of the personnel and considered as odd or suspicious activity, which leads to the highest risk score. The Ants and Pathfinder model both put efforts on education a motivation, but they are both "given from the outside" and the Ants model with "foreign twist" may cause slightly more resistance to change than homemade Pathfinder model. The Strength of the Mule model relays on building a stable organizational culture with time and involvements of the participants to the development with AI. Scores: Mule 1, Pathfinder 2, Ants 3 and Turtle 4.

Risks related to legal and ethical issues are based on building blocks labeled with Legal and Learn. The Pathfinder model takes deliberate high risks with considered objects and gets the risk score of 4. Oppositely, the Turtle model avoids these risks and the risk score is 1. In the middle, the assets with international cooperation make Ants model a little better than the Mule model, so the Ants model gets risk score of 2 and the Mule model gets 3.

The risks related to Leading are assessed by the clarity of responsibility, commitment and motivation. With the Turtle model the structure is clear and delegating and sharing of responsibilities is easy. The goal-oriented Pathfinder comes as a second despite the challenging parallel activities. The Mule model suffers from the same challenges but without decisive activities in leading and it is therefore

placed in the third place. The management of the risks in the multinational projects are considered to be more demanding compared to the other models[71].

The risks related to Skills are assessed by the existence of expertise and allocation in time in the models. The quality and quantity of expertise is greatest with the Ants model. The Pathfinder starts acquiring expertise from the early beginning while the Mule model concentrates on that later. The Turtle model has the highest risk score because the late-born expertise has its vast disadvantages, at least according to the Brook's law[72].

On the next aspect of capability, the risks with the tools are connected to the building blocks labeled as Project and Agility. This risk has a near relationship to Skills, but here the focus is on the hardware and software rather than skills of using these tools. The early investments raise the Ants model to pole position. The Pathfinder is in the second place while the Mule and Turtle models are the last positions suffering from the late investments.

Lack of collection of data is the next capability risk. The intensity and the starting time of activity are key aspects of this assessment. The Pathfinder model prioritizes the collection of data and is therefore assessed with the lowest risk score. The Ants model is for the same reason in the second-lowest position while the Mule and Turtle models are the last positions again suffering from the late activities.

The last risk is about the inadequate support for the development work. The investments to the building block labeled with the Cradle plays a vital role in the assessment. The Ants model benefits from the early start and resources from multinational collaboration. For similar reasons, the Pathfinder model becomes second, the mule model third and the Turtle model last.

This assessment is done with deductive reasoning and questions considering objectivity may rise. To increase the objectivity of this assessment it is highly recommended to use expert-oriented methods like the Delphi technique in further studies. If the Delphi is used, it is important to gather the panel of experts with extensive representation from both inside and outside the organization. The development and implementation of other conceptual models are also recommended.

7.5 Summary of the comparison

The summary of the comparison is presented in the following table. It is essential to remember that the achieved results are representing just a model of assessment. Lack of objectivity in this assessment and restrictions, like missing weights and use of ordinal metrics, should be mentioned when these results are presented later.

RISK	TURTLE	PATHFINDER	MULE	ANTS
GAP	4	2	3	1
CONTROL	1	3	4	2
WASTE	3	4	1	2
TRUST	4	2	1	3
LEGAL/ETHICS	1	4	3	2
LEADING	1	2	3	4
SKILLS	4	2	3	1
TOOLS	4	2	3	1
DATA	4	1	3	2
SUPPORT	4	2	3	1
TOTAL SCORE	30	24	27	19
HIGHEST RISK	1.	3.	2.	4.

Table 8: Summary of the comparison without weights

In this case the Turtle model seems to have the highest risk and the Ants model seems to be the most appropriate model to adopt for further work, but the more thorough research is needed in order to get valid results, and similar approach with Soft System Methodology is highly recommended.

According to these results, some risks tend to interact with others. The enablers, like Skills, Tools and Support seem coherent. Likewise, Legal/Ethics and Control are nearly the same. A more detailed consideration, for example with the mathematical calculation of variance, is pointless, because of the accuracy limitations mentioned earlier.

Despite the limitations with the achieved results, there seems to be some patterns of features that can be identified. Successful models put efforts into the collection of data, agility, monitoring and experimental platforms as soon as possible. All of these are a prerequisite for launching AI-related projects, and delays reflect poorer results. The front-weighted models seem to gain better results, and this is visualized into the next picture.

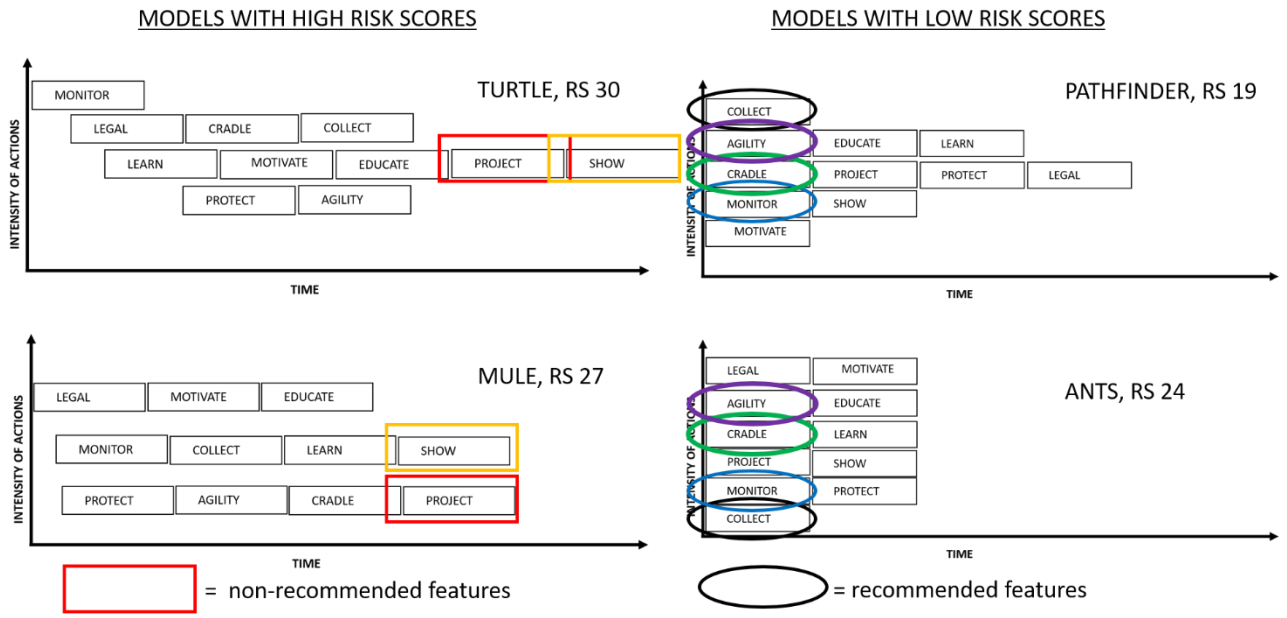

Figure 16: Models and Patterns

The research method, soft system methodology, emphasizes similar features than for example, the AI Canvas model[73]. Identifying customers, stakeholders, needed data and skills are presented in te same way in this and the Canvas model. Integration in the Canvas model is a part of Leading in this Research. The Cost and the Revenue in the Canvas model has similarities compared to the risk of unproductive investment in this study. The connection between the risk of Gap in this study and the Output and Value Proposition in the Canvas model is undirect - the risk of Gap has a straight connection to the capability requirements and filling these are measured with metrics which are referred in the Output of the Canvas model. If the formation of the gap is prevented the activities can be considered in accordance with the values.

All the presented conceptual models have their pros and cons and choosing one of them or any other has a huge importance for developing military capabilities with Artificial Intelligence in the future. The next step with the Soft System Methodology is to define possible changes, but these are strongly related to the chosen conceptual model. While this decision is not made, there is still a possibility to identify general key factors for success. These factors are converted to recommendations, presented in the next section.

7.6 Recommendations for the real-world

The real-world is full of limitations, while the development of AI seems to open doors of new opportunities in ever-increasing speed. At the same time, the current global health crisis will affect the world economy for a long time[74], and funding of changes, which does not support the fight against Corona-virus, will be difficult to obtain. This is the reason why the following recommendations are strongly based on cost-effective solutions.

The data remains as an important raw material for the AI development and all the means that increase collection of data is highly recommended according to this research. Circumstances prefer collecting different kinds of data in Finland – and among others, four seasons and varying weather conditions generate versatile multidimensional data and millions of mobile devices in the hands of educated people enable capturing it. Civilians can play a vital role in capturing the Big Data, but the military personnel should also be encouraged to invent new ideas of collecting different kinds of data, simulate or real. For example, military vehicles and vessels are suitable platforms for data collection – offering mobility, protection, human-machine interaction and power sources for sensors and computers, thus enabling the later development of machine learning and autonomous functions.

The necessary arrangements to receive, store and manage data create the basis of the second recommendation – improve the capability to store and share data. There is no point to collect data if it cannot be fully utilized later. The increasing amount of data emphasizes the modularity so that the storage can expand over time. This subject has various aspects to cover, but the planning and building of this capability should not slow down the start of data collection. Implementing an iterative and incremental framework for managing this complex work, like Scrum, might offer an interesting kick-start to train agility. On the other hand, this is not in the core of military activities, so the possibilities of mapping the long-term strategic partnerships should be prioritized.

The third recommendation is to boost the training of agile methods with the experimental projects. Participating people learn by doing, knowledge and experience will increase and the readiness to develop concepts and counter-weapons will remain up-to-date. The new ways of collaboration between national and international stakeholders, like universities, research agencies and defence industry, support the launching of the bold and novel projects. New projects should provide both a scientific challenge and an opportunity to the industrial partners, meaning that the projects should be targeted at the identified military areas without previous business, which is controversial to the idea of investing in only battle-proven material. This leads to the fourth recommendation – how to pave the way for this.

The fourth recommendation based on this research is to tune-up organizational culture to match the future! Finding new ways to motivate, educate and train people are essential when creating a climate for change, likewise in the Kotter´s 8-step change model. All stakeholders should understand that the failures and drawbacks in AI-projects are allowed and just a natural part of the overall development. Today's failure might be the cornerstone in building tomorrow's capability.

The last recommendation is to keep on monitoring the development of AI, because that is the only early warning system there is. National and international collaboration is highly recommended in both activities based on the findings of this research.

These recommendations are valid with any of the presented conceptual models.

8 THROUGH DISCUSSION TO CONCLUSIONS

In this chapter, the essential findings of this study are discussed, and the final conclusion is presented. The discussion includes suggestions for further research and criticism considering different aspects of this study.

The first task of this study was to focus on answering the question - why the Finnish Defence System should prepare for the development of Artificial Intelligence? According to this study the FDF has a legal obligation to maintain an adequate defence in all dimensions. Dimensions are protected with the capabilities and to prevent future capability gaps, the defence system should be updated to face the major changes in the future. The scope of AI-related research is expanding, and the volume of the potential AI-users is already huge according to the sources of this study. This indicates that the Artificial Intelligence, as an emerging technology field, can and will provide opportunities and risks for the development of future defence system. To manage these risks, the FDF is obligated to prepare for the development of Artificial Intelligence.

The second task of this study was creating a systematic view on the Finnish defense system together with the aspect of AI development. With the documentary analysis and using the Soft System Methodology this was possible. The accuracy of the view depends on the sources used, and by using open sources, some of the smaller details were lost. This did not prevent the further use of Soft System Methodology, which focuses more on the processes and less for the details. This also offered a possibility to approach the future systemically and thus covering the third task. To maintain objectivity in this study, no external assessments, like trend lists or hype curves, of the future details in AI development were presented, but examples of means and risks of assessments were included.

The fourth task was focusing on defining the opportunities and threats. The used main method, the Soft System Methodology, emphasizes the generating of general root definitions, implementation of conceptual models, and comparison between them, rather than identifying single risks or opportunities. Through the comparison the essential risk areas were identified but the opportunity areas did not reveal themselves in the same way. Further research on finding the possible opportunity areas is highly recommended but not with this main method. For example, the utilization of the Canvas method for this might be worth exploring, but it is important the remember the true nature of the defence system – it provides security in a cost-effective way, and seeking for the business opportunities is not in the core of the system. The last task of this study was wrapping up the major findings and answer the main question with the help of deductive reasoning. The following recommendations are the essence of this study:

- the organization should increase the intensity of collecting data
- the organization should improve the capability to store and share data
- the organization should boost the training of agile methods with the experimental projects
- the organization should tune-up organizational culture to match the future
- the organization should keep on monitoring the development of AI

The scope of this study was specific and any previous research emphasizing the similar aspects was not found during this study. The nearest governmental-oriented approach was from the government of the United Kingdom, which share a guide collection online focusing on 1.) general understanding of AI, 2.) Assessment if the AI is a right solution, 3.) planning and preparing for AI implementation and 4.) Managing AI project. After the benchmark, it seems that this set of guides shares many of the findings of this study, but some areas, like risk management, are presented just as a useful way to consider. There are many good details in this guide that deal with AI and getting to know it is recommended.

The invention of nuclear power did not launch the technological revolution or the major change in the military capabilities – it was the people who decided where and how to use that novel idea. In the same way, Artificial Intelligence is not going to launch a revolution or at least so we would like to hope for the sake of human mankind in the future. The people, us, we make the decisions. It is vital to decide now in which role we want to play if the AI revolution happens. Are we going to be victims or bystanders of that revolution or are we going to be a part of that revolution? This research reveals the first steps for the Finnish Defence Forces or any other similar process-based organization to embrace an active role in the future development of Artificial Intelligence.

This study concludes that the new brains for the defense system do not mean changing the human brains for artificial – it means the updating of the human minds now to take an active role in the possible AI revolution in the future.

9 APPENDIX – CATWOE FRAMEWORK

CATWOE MODEL	
Customer	Who or what is affected by the change?
Actor(s)	Who performs the necessary activities?
Transformation	What is the single activity or process that makes transformation?
Worldview	What is the view which makes the transformation worthwhile?
Owner	Who is responsible to make changes happen?
Environment	Which environmental issues are worth considering?

Root definition 1: identify and focus on the utilization of artificial intelligence in the development of military capabilities.	
Customer	Main process 1: capability plan and development
Actor(s)	Personnel of main process 1, Defence Intelligence Agency, Defence Research Agency
Transformation	Create a situational picture of the present and future (foresight) AI innovations and share the information with defined stakeholders.
Worldview	"The world is changing dynamically - innovations are meant to be exploited"
Owner	Owner of main process 1
Environment	There are accessible and non-accessible information and disinformation

Root definition 2: identify existing data in the daily activities, create or improve means to collect it and share the information of the gathered data.	
Customer	All personnel and strategic partners
Actor(s)	The Personnel Division of Defence Command Finland, National Defence University, The Finnish Defence Forces Logistics Command
Transformation	Train all personnel to participate in change and make it possible by collecting data
Worldview	"People want to develop and be part of something bigger"
Owner	Commander of the Finnish Defence Forces
Environment	Solving the open questions of security is a prerequisite for development

Root definition 3: ensure that the required level of education in AI is achieved and updated to all personnel in regularly bases.	
Customer	All personnel and stakeholders
Actor(s)	The Personnel Division of Defence Command Finland, National Defence University
Transformation	Define different levels of required competence and organize training
Worldview	"Change is possible and obedience in the organization enables it."
Owner	Commander of the Finnish Defence Forces
Environment	Resistance to the change due to ignorance will hamper the development

Root definition 4: re-evaluate recruiting strategy and create AI positive organization culture.	
Customer	New staff to be recruited and existing personnel of FDF
Actor(s)	The Personnel Division of Defence Command Finland, National Defence University
Transformation	Create new career paths and encourage employees to enlarge their knowledge of AI
Worldview	"Satisfied and motivated employees produce more"
Owner	Owner of main process 1: service activities
Environment	It will take years to build a new organizational culture, but AI is evolving at an accelerating pace alongside – immediate actions are needed.

Root definition 5: approve a certain level of uncertainty and make necessary commitments for agile activities with AI.	
Customer	All personnel and stakeholders
Actor(s)	Personnel of main process 1, Finnish Defence Research Agency
Transformation	Develop new agile process frameworks and methods to manage complex AI projects and start piloting as soon as possible
Worldview	"Old foundations do not support the development of new structures"
Owner	Owner of main process 1
Environment	Experimental development requires resources and long-term commitments from all the stakeholders. There will be more quick-loses than quick-wins.

Root definition 6: should reflect the AI excellence of the organization with state-of-the-art service systems.	
Customer	Users of service systems
Actor(s)	Personnel of main process 4, Shared Service Centre
Transformation	Develop AI applications that run on existing data for administrative use to build trust and achieve experience before shifting to the more demanding systems.
Worldview	“The more You succeed, the more You want to succeed, and the more You find a way to succeed. “
Owner	Owner of main process 4
Environment	There will be many challenges but that must be accepted with the pioneers.

Root definition 7: establish new AI-oriented platforms and means to enhance collaboration with various of stakeholders.	
Customer	Main process 1: capability plan and development
Actor(s)	Owner of main process 1, Defence Research Agency
Transformation	Present new ways of collaboration and data management and create experimental platforms for innovative thinking and testing
Worldview	“Opportunities don't happen – they are made in creative environments”
Owner	Owner of main process 1
Environment	A creative environment doesn´t mean new organizations or resources, it is more likely a mind-set of productive thinking and sharing thoughts.

Root definition 8: invest in AI-related research and innovation which support the development of military capabilities.	
Customer	Personnel of main process one, Defence Research Agency, stakeholders
Actor(s)	Main process 1: capability plan and development
Transformation	With experimental projects achieve proof of concepts for further development with strategic partners and other identified stakeholders.
Worldview	“Proceed boldly to the unmapped areas and prepare to guide the others”
Owner	Owner of main process 4
Environment	More intensive co-operation with national and international stakeholders is needed to cover different research areas.

Root definition 9: track the environment for any signs and effects of use of Artificial Intelligence.	
Customer	Decision makers at all levels and defined stakeholders
Actor(s)	Main process 3, Defence Intelligence Agency, Defence Research Agency
Transformation	Create proactive AI-early-warning systems for all dimensions and investigate the cause-and-effect relationships.
Worldview	"If you want peace, prepare for war"
Owner	Owner of main process 3
Environment	To cover the external threats on the whole environment an international co-operation is needed. For internal threats, the responsibility of developers should be clarified.

Root definition 10: be aware of the instructions and restrictions and follow them.	
Customer	All personnel and stake holders
Actor(s)	Defence Command Legal Division
Transformation	Participate international work with AI related legislation and ensure that pre-requisites for AI development enable work for defensive purposes
Worldview	"Pursuit for the good of humanity, but don't trust the goodness of the people"
Owner	Assessor of the Finnish Defence Forces
Environment	Quick and easy solution is to stop all development of AI with international legislation, but "de facto" development continues in classified programs. Defining the balance between legislation and development for defensive purposes is the key factor of success.

Root definition 11: fortify the defence of the cyber and info dimension	
Customer	All personnel and stakeholders
Actor(s)	Main process 1: capability plan and development
Transformation	Identify present and future threats related with AI and update systems with necessary means.
Worldview	"Data is the new currency – take care of it likewise with the yesterday's money"
Owner	Owner of main process 1
Environment	Interests of different governmental and non-governmental organizations and activities of individuals towards data is increasing. Pinpointing the counter-measures will become more and more challenging.

10 SOURCES

[1] Joshua Yeung, "Three Major Fields of Artificial Intelligence and Their Industrial Applications", Towards Data Science, https://towardsdatascience.com/three-major-fields-of-artificial-intelligence-and-their-industrial-applications-8f67bf0c2b46, [accessed 6-April-2020]
[2] Anita Rubin, "Tulevaisuudentutkimus tiedonalana", Turun Yliopisto -tulevaisuuden tutkimuskeskus, https://tulevaisuus.fi/perusteet/tulevaisuudentutkimus-tiedonalana/[accessed 6-April-2020]
[3] Yuval Noah Harari," Lessons *for the 21st Century"*, Spiegel & Grau, Jonathan Cape, August 2018, pp 209-210.
[4] Joe Carmichael, "Elon Musk says DARPA A.I hacking challenge will lead to SKYNET", https://www.inverse.com/article/18301-elon-musk-warns-that-darpa-artificial-intelligence-security-challenge-will-yield-skynet, [accessed 6-April-2020]
[5] Peter Checkland," Systems *thinking, systems practice", Wiley & sons, 1981*
[6] Skillsyouneed.com, https://www.skillsyouneed.com/learn/dissertation-methodology.html, [accessed 7-April-2020]
[7] Act on the Defence Forces 11.5.2007/551, Chapter 1 2§ "*The duties of the Defence Forces"* https://www.finlex.fi/fi/laki/ajantasa/2007/20070551, [accessed 6-April-2020]
[8] The Personnel Division of Defence Command, "*Henkilöstötilinpäätös 2017", Juvenes Print 2018,* https://puolustusvoimat.fi/documents/1948673/2267037/PEVIESTOS_Henkilostontilinpaatos_2017/aef7c602-f7fc-4440-893f-54799f35918a/PEVIESTOS_Henkilostontilinpaatos_2017.pdf, [accessed 6-April-2020]
[9] Plans and Policy Division Defence Command, PVOHJEK-PE, PVOHJEK-PE "*Puolustusvoimien prosessiohjaus*", HK262, 22.8.2014.
[10] Defence Acquisition University, https://www.dau.mil/acquipedia/pages/articledetails.aspx#!457, [accessed 6-April-2020]
[11] Jukka Anteroinen," Enhancing *the Development of Military Capabilities by a Systems Approach",* National Defence University, Department of Military Technology, *Series 1: Publication No. 33, Juvenes* Print 2013, pp.16-19.
[12] Ministry of Defence, "*Comprehensive National Defence*", https://www.defmin.fi/en/tasks_and_activities/comprehensive_national_defence, [accessed 6-April-2020]
[13] Iyad Rahwan etc., "Machine Behaviour", Nature, April 2019, https://www.nature.com/articles/s41586-019-1138-y, [accessed 6-April-2020]
[14] Yaval Noah Harari: "*A Brief History of Humankind"*, Random House 2011
[15] Geoffrey Regan: "*Great Military Blunders*", Carlton 1991
[16] Boyd, John R, "*Destruction and Creation* "(PDF). U.S. Army Command and General Staff College, 1976
[17] Altpro D.O.O: " *Dead man´s switch"* http://www.btobrail.com/administration/moxiemanager/data/files/INFRASTRUCTURE/ALTPRO/AP_A3_company_letter.pdf, [accessed 8-April-2020]
[18] Heikki Ailisto etc, *"Tekoälyn kokonaiskuva ja kansallinen osaamiskartoitus – loppuraportti"*, VALTO 2019, http://urn.fi/URN:ISBN:978-952-287-632-4 , [accessed 8-April-2020]
[19] Kasey Panetta, " *Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017*" Gartner, https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/, [accessed 8-April-2020]
[20] Kirsten Gronlund, " *State of AI: Artificial Intelligence, the Military and Increasingly Autonomous Weapons* ", Future of Life Institute, 2019, https://futureoflife.org/2019/05/09/state-of-ai/?cn-reloaded=1, [accessed 8-April-2020]
[21] Prime Minister's Office Publications, "*Government's Defence Report 7/2017*", Lönnberg print & promo, 2017, https://www.defmin.fi/files/3688/J07_2017_Governments_Defence_Report_Eng_PLM_160217.pdf, [accessed 8-April-2020]
[22] Jean Thoma, "*Energy, Entropy and Information*", 1977 http://pure.iiasa.ac.at/id/eprint/783/1/RM-77-032.pdf,[accessed 8-April-2020]
[23] Alberts, David S.; Garstka, John J.; Stein, Frederick P., "*Network centric warfare: developing and leveraging information superiority*" , 1999, *Network centric warfare : developing and leveraging information superiority*, http://dodccrp.org/files/Alberts_NCW.pdf, [accessed 8-April-2020]
[24] Richard D.Hooker, jr, "*21st Century Doctrine and Future of Maneuver*", 1991, https://www.ausa.org/sites/default/files/LWP-8-21st-Century-Doctrine-and-the-Future-of-Maneuver.pdf, [accessed 8-April-2020]

[25] Rafael Moreira Savelli, Gustavo Henrique Soares de Oliveira. Lyrio Roberto de Beauclair Seixas, " *The Maneuver and attrition warfare – Simulation system* ", 2004, https://www.marinha.mil.br/spolm/sites/www.marinha.mil.br.spolm/files/arq0061_0.pdf, [accessed 8-April-2020]
[26]Roger Molander, Andrew Riddile, Peter Wilson, " *Strategic Information Warfare- The new Face of War", RAND, 1996,* https://apps.dtic.mil/dtic/tr/fulltext/u2/a306977.pdf, [accessed 8-April-2020]

[27] Osmo Kuusi, Timo Bergman & Hazel Salminen (toim.) Miten tutkimme tulevaisuuksia? – kolmas, uudistettu painos / Jarl-Thure Eriksson: ”*Kaaosteoria ja kompleksisten järjestelmien hallittavuus*”, Vammalan kirjapaino 2013.
[28] Wang, R.; Strong, D, "*Beyond Accuracy: What Data Quality Means to Data Consumers*". *Journal of Management Information Systems*.1996 **12** (4): 5–34. doi:10.1080/07421222.1996.11518099, [accessed 8-April-2020]
[29] Kamiz E. Maani, Robert Y. Cavana: ”*Systems methodology*”, thesystemsthinker.com, https://thesystemsthinker.com/systems-methodology/, [accessed 8-April-2020]
[30]Ricardo Rodriguez-Ulloa & Alberto Paucar-Ceceres, ” *Soft System Dynamics Methodology (SSDM): Combining Soft Systems Methodology (SSM) and System Dynamics (SD)*”, SpringerLink, https://link.springer.com/article/10.1007/s11213-005-4816-7, [accessed 8-April-2020]
[31] Theodore Rockwell, ”The Rickover Effect: How One Man Made A Difference”, Naval Institute Press, 1992.
[32] Mss Defence: ” *Combat Management Systems*”, https://www.mssdefence.com/blog/combat-battle-management-systems/, [accessed 8-April-2020]
[33] Vincent Boulanin & Maaike Verbruggen, ” Mapping the development of autonomy in weapon systems”,SIPRI, 2017, ”https://www.sipri.org/sites/default/files/2017-11/siprireport_mapping_the_development_of_autonomy_in_weapon_systems_1117_1.pdf, [accessed 8-April-2020]
[34] Air Force Technology, ”*X-45 J-UCAV (Joint Unmanned Combat Air System)”,* https://www.airforce-technology.com/projects/x-45-ucav/, [accessed 8-April-2020]
[35] Chee Khiang Pang, Akash Kumar, Cher Hiang Goh, Cao Vinh Le, “*Nano-satellite swarm for SAR applications: design and robust scheduling*”, IEEE, 2015, https://ieeexplore.ieee.org/abstract/document/7126148, [accessed 8-April-2020]
[36] SAP SE, ”Leonardo”, 2019, https://www.sap.com/products/leonardo/machine-learning.html, [accessed 8-April-2020]
[37] Hosomi Itaru, ” *The Potential of AI to Propose Security Countermeasures*”, NEC Technical Journal, 2017, https://www.nec.com/en/global/techrep/journal/g17/n02/170216.html, [accessed 8-April-2020]
[38] Naveen Joshi, ”*4 Ways Global Defense Forces Use AI*”, Forbes, 2018, https://www.forbes.com/sites/cognitiveworld/2018/08/26/4-ways-the-global-defense-forces-are-using-ai/, [accessed 8-April-2020]
[39] Niklas Mashur, “*AI in Military Enabling Applications*”, CSS, 2019, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse251-EN.pdf, [accessed 22-April-2020]
[40] John Kotter, ”*Leading Change*”, Harward Business Review Press, 2012
[41] Gennady Shkliarevski, ” *How We Should Respond to the AI Revolution*”, International Policy Digest, 2018, https://intpolicydigest.org/2018/10/03/how-we-should-respond-to-the-ai-revolution/, [accessed 8-April-2020]
[42] Internet Society, “*Artificial Intelligence and Machine Learning: Policy Paper”, 2017,* https://www.internetsociety.org/resources/doc/2017/artificial-intelligence-and-machine-learning-policy-paper/?gclid=Cj0KCQjws_r0BRCwARIsAMxfDRiEaVEAW-LmD7MyQPtjQqlkzPxhri5eOcqPSgeUVafn4LPx6jYEGXUaAv5cEALw_wcB, [accessed 22-April-2020]
[43] Sameer Sharma, “*Harnessing the fruits of the AI revolution*”, PluriConseil, 2020, https://www.pluriconseil.com/harnessing-the-fruits-of-the-ai-revolution/, [accessed 12-April-2020]
[44] Kaja Polachowska, “*12 challenges of AI adoption*”, Neoteric, 2019, https://neoteric.eu/blog/12-challenges-of-ai-adoption/, [accessed 22-April-2020]
[45] Cogito Tech LLC, “*Where is Artificial Intelligence Used Today?”,* medium.com, 2019, https://becominghuman.ai/where-is-artificial-intelligence-used-today-3fd076d15b68, [accessed 12-April-2020]
[46] Ana Bera, “*Is Siri Better Than Google? – 16 Interesting Siri Statistics*”, SafeAtLast, 2019, https://safeatlast.co/blog/siri-statistics/#gref, [accessed 22-April-2020]
[47] Statista, “Number of Netflix streaming subscribes worldwide”, 2019, https://www.statista.com/statistics/250934/quarterly-number-of-netflix-streaming-subscribers-worldwide/, [accessed 22-April-2020]
[48] Kambria, “*How Facebook Uses Artificial Intelligence*”, 2019, https://kambria.io/blog/how-facebook-uses-artificial-intelligence/, [accessed 22-April-2020]
[49] 99Firms, “Google Search Statistics”, 2020, https://99firms.com/blog/google-search-statistics/#gref, [accessed 22-April-2020]
[50] Bankmycell, “How many smartphones are in the world?”, bankmycell.com, 2020, https://www.bankmycell.com/blog/how-many-phones-are-in-the-world, [accessed 22-April-2020]
[51] Rodney Brooks, “*The Seven Deadly Sins of AI Predictions*”, MIT Technology Review, 2017, https://www.technologyreview.com/2017/10/06/241837/the-seven-deadly-sins-of-ai-predictions/, [accessed 22-April-2020]
[52] Michael Echols, “*Uncertainty Is the Future Certainty*”, ChiefLearningOfficer, 2019, https://www.chieflearningofficer.com/2019/04/16/uncertainty-is-the-future-certainty/, [accessed 23-April-2020]
[53] Luke Georghiou, Jennifer Cassingena Harper, Michael Keenan, Ian Miles and Rafael Popper, “The Handbook of Technology Foresight”, Edward Elgar Publishing Limited, 2008.
[54] Vikram Karve: ” *ROOT DEFINITION & CATWOE MODEL - Ethics Based Soft Systems Approach*”, http://karvediat.blogspot.com/, 2010, http://karvediat.blogspot.com/2010/10/root-definition-catwoe-model-ethics.html, [accessed 12-April-2020]
[55] Susan Gasson, ”*Root Definitions & Conceptual Models*”, Improvising Design, https://blog.improv-design.com/soft-systems-methodology/root-definitions/, [accessed 12-April-2020]

[56] Government Digital Service and Office for Artificial Intelligence / UK," *A guide to using artificial intelligence in the public sector*", 2019, [accessed 12-April-2020]
[57] lausuntopalvelu.fi, "Luonnos valtioneuvoston selonteoksi - Eettistä tietopolitiikkaa tekoälyn aikakaudella", 2018, https://www.lausuntopalvelu.fi/FI/Proposal/ShowAllProposalAnswers?proposalId=f05b7eb2-ff3b-4fc0-a5f7-89ee30975cbb, [accessed 12-April-2020]
[58] Roger Atkinson," *Project management: cost, time and quality, two best guesses and a phenomenon, its time to accept other success criteria*", International Journal of Project Management, 1999, https://www.sciencedirect.com/science/article/abs/pii/S0263786398000696?via%3Dihub, [accessed 15-April-2020]
[59] International Organization for Standardization," *Risk management — Guidelines*", ISO 31000:2018, 2018, https://www.iso.org/standard/65694.html, [accessed 15-April-2020]
[60] Max Tegmark, " *Benefits risks of Artificial Intelligence*", Future of Life Institute, 2016, https://futureoflife.org/background/benefits-risks-of-artificial-intelligence/, [accessed 17-April-2020]
[61] Sabine Roeser etc," *Handbook of Risk Theory",* Springer 2012
[62] High-Level Expert Group on AI," *Ethics guidelines for trustworthy AI*", European Commission, 2019, https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai, [accessed 17-April-2020]
[63] Robert.C.Martin, "*Agile Software Development*", Pearson, 2002.
[64] Adrien Book, "*10 Steps to your very own Corporate A.I project*", Towards Data Science, 2019, https://towardsdatascience.com/10-steps-to-your-very-own-corporate-a-i-project-ced3949faf7f, [accessed 18-April-2020]
[65] Seremba John Paul, "*How to successfully lead a Software Development Team*", The Andela Way, 2018, https://medium.com/the-andela-way/how-to-successfully-lead-a-software-development-team-6b9a6ffcf760, [accessed 18-April-2020]
[66] Daniel Greenberg, " *What Skills Do You Need on an AI Project?",* Excella, 2019, https://www.excella.com/insights/what-skills-do-you-need-on-an-ai-project, [accessed 18-April-2020]
[67] Jessie Leung,"*The Benefits of Pair Programming*", Better Programming, 2019, https://medium.com/better-programming/when-pair-programming-works-it-works-really-well-heres-why-c51857bbcf0f, [accessed 18-April-2020]
[68] Tim Worstall, " *If data really is the new oil, the raw materials need a different economic approach*", Computer-Weekly.com, 2019, https://www.computerweekly.com/opinion/If-data-really-is-the-new-oil-the-raw-materials-need-a-different-economic-approach, [accessed 18-April-2020]
[69] AIMultiple: " *Data labeling/ annotation/ classification in 2020: In-depth Guide*", 2020, https://blog.aimultiple.com/data-labeling/, [accessed 18-April-2020]
[70] Wiktor Schmidt," *Lesson Learned: Working with Teams Across Borders*", Netguru, 2014, https://www.netguru.com/blog/lesson-learned-working-with-teams-a, [accessed 18-April-2020]
[71] Kirsi Aaltonen, Mervi Murtonen & Sampo Tukiainen," *Three perspectives to global projects Managing risks in multicultural project networks*" VTT, 2009, https://www.vttresearch.com/sites/default/files/pdf/tiedotteet/2009/T2491.pdf, [accessed 18-April-2020]
[72] Fred Brooks," *The Mythical Man-Month*", Addison-Wesley, 1975.
[73] Jan Zavadzki, " *Introducing the AI Project Canvas*", Toward Data Science, 2019, https://towardsdatascience.com/introducing-the-ai-project-canvas-e88e29eb7024, [accessed 20-April-2020]
[74] Arthur Sullivan," *As the coronavirus triggers a global economic crisis, just how bad could it get?",* DW, 2020, https://www.dw.com/en/as-the-coronavirus-triggers-a-global-economic-crisis-just-how-bad-could-it-get/a-53000638, [accessed 20-April-2020]