The Finnish Defence Forces' Research Agenda 2015

Table of contents

Objective and target group

The Finnish Defence Forces' research agenda outlines research needs based on observed changes in the operating environment and the new challenges that the Defence Forces is facing.

The research agenda is not intended to be a plan that defines specific research tasks, their schedules or resources. Instead, it addresses areas of interests and broad research themes based on the long term needs in which the Defence Forces seek to enhance research cooperation with the scientific community, industry as well as governmental agencies at both the national and international level.

The target group of the research agenda consists of, on the one hand, the Defence Forces' research staff, who plan and carry out national and international research cooperation, and on the other hand the scientific community and industry, which are capable of producing expertise and innovations related to the Defence Forces' tasks in the fields described in the agenda. The agenda may also prove useful to other authorities who contribute to the provision of society's security.

The research agenda supports innovative development by helping direct attention to the areas considered crucial for the long-term development of the Defence Forces.

The defined research themes are central for the development of the defence system, and each of them has its own information needs. Fulfilling these needs necessitates interdisciplinary research and development ranging from the humanities to natural sciences. The phenomena related to these themes are examined broadly, covering personnel, materiel, doctrine, organisation and information. The agenda helps clarify how these individual research themes are connected to each other and the overall development of the Defence Forces.

The research agenda describes the phenomena that the Defence Forces considers the most important over the course of the next 15 years. It is clear that over this period of time the operating environment will be under a constant process of change. In order to be able to make strategic decisions that also take future development into consideration, the Defence Forces must study, be aware of and prepare to respond to the changes. This is of utmost importance when making decisions related to how we develop our future capabilities.

Key phenomena

- Evolving operating environment and changes in the nature of crises and warfare
- The person as part of systems and units
- Information operations
- Networking
- Capability in the electromagnetic spectrum
- Systems with autonomous characteristics

The research agenda consists of six different phenomena, each of which is considered vital for the future of the Defence Forces in their own way. Of these phenomena, changes in the operating environment and the nature of crises and warfare, the person as part of a system and a unit, and information operations are very broad themes, while networking and autonomy are somewhat narrower in scope. Meanwhile, capability in the electromagnetic spectrum is a clearly technology-based theme.

Evolving operating environment and changes in the nature of crises and warfare

Today's operational environment is in flux. Changes in the global security environment coupled with increasingly rapid technological development challenge our perception of war and warfare as well as how we define the role and use of the armed forces.

The current security environment is characterised by increasing interdependencies and the emergence of new actors. Different geographic areas, nations and non-state actors have been bound together by information flows as well as trade and economic networks. In the midst of the changes affecting the international system, non-state actors have, by utilising global networks, challenged the traditional state-centric international system and its structures.

As geographical and physical distances have begun to lose their meaning, the security threats emerging from the security environment have expanded and multiplied. In the current interdependent security environment, disturbances may have unexpected consequences, which are reflected in the regional and local level while also affecting the security of Finland.

Although the use of force has maintained its role as one of the key feature in the international system, the changes in the global security environment coupled with increasingly rapid technological development have challenged the traditional view on how we define war and warfare as well as the role of the armed forces and their operational concepts.

The increasing complexity of conflicts, the emergence of new actors and the expanding range of operating methods have blurred the line between war and peace. Recent conflicts have been characterised by the convergence of kinetic and non-kinetic methods, which are used to comprehensively influence society, its citizens and the military. Military force is applied in an increasingly coordinated and coherent manner with economic, political and information-based methods of influence.

Technological development has enabled the utilisation of advanced weapons systems that affect targets with precision-guided munitions and can be deployed even from great distances away from the actual operation area. At the same time, interoperability has become a necessity. Military operations are being conducted in the form of multinational joint operations ranging from high intensity operations to humanitarian crisis management.

These operations are characterised by a high operational tempo and the adversary's use of asymmetrical tactics, which all set new requirements for the operation of both the individual soldier and groups of soldiers. After all, the soldier is an integral part of this battle space consisting of various systems and networks, in which key success factors include quick adaptation to the situation, decision-making ability and the creative application of tactical thinking. The changing nature of war and warfare sets new requirements for soldiers' physical and mental performance, which must be considered in both training and selection procedures.

The Defence Forces' operating environment is under constant change on all levels, demanding continued research into the changing nature of war and warfare on the strategic, operational and tactical levels. Thus the forecasting as well as the identification of trends and innovations are key elements in the process of developing the future capabilities of the Defence Forces. It is critical to acknowledge that this development can only be understood and utilised through comprehensive and multidisciplinary research. As such, the Defence Forces' research activities must focus increasingly on national and international networking with universities, research institutes, industry and other government operators.

The person as part of systems and units

In future conflicts, soldiers operate in an increasingly complex and chaotic environment, which is extremely taxing both physically and mentally. During operations, a soldier must be able to interact with people from different cultural backgrounds. Due to the changing nature of crises, war is fought not only against an adversary but also increasingly on the level of ideas, and under media pressure.

This multidisciplinary research theme centres around human performance in its entirety, the human-machine interface, as well as learning.

A soldier must be able to operate responsibly in changing, complex, taxing and unpredictable situations and environments. This is called human performance, which consists of physical, mental, ethical and social performance. These can be affected and developed through training, exercise, guidance, medical procedures and new technologies. The objective is – depending on the individual's initial level – to mend and restore, preserve and maintain or improve and enhance human performance.

Physical performance includes nutrition, rest, environmental health and fitness optimisation as well as service safety, including carried and worn equipment.

Due to the changing nature of war and warfare, the soldier of the future must be increasingly able to mentally cope in areas under hostile control and otherwise under hostile influence. Mental performance includes the development of cognitive skills and the acknowledgement of aptitude assessment in personnel assignment, as well as developing a sense of competence, motivation and national defence will. Human performance is maintained through the improvement of stress tolerance and resilience and, as a last resort, through medicinal means. When assessing the mental performance of professional soldiers and reservists, changes in society must also be taken into consideration.

Measures for supporting physical and mental performance include the identification and prevention of health risks, military medical treatment and preventive medicine as well as patient evacuations and field medicine. Technological development introduces new opportunities in these fields as well, for example in the form of remote or precision medication and physical status monitoring.

Decision-making in a changing operating environment under an increasingly rapid operating tempo requires good ethical performance. An ethically capable soldier knows the significance of cultures, religions and conventions, and knows how to utilise military pedagogy. Cultural awareness also touches upon social performance, which consists of interaction behaviour, group cohesion, socio-cultural norms as well as values and attitudes.

The increasing functionality and intelligence of machines emphasises the ways in which people and machines can support each other. The key to creating a functional system is taking human factors into consideration from both the human and machine perspective. Key factors related to the human-machine interface – and, overall, human system integration – include ergonomics, embedded information technology, wearable electronics and smart clothes, augmented or mixed reality, physical status monitoring and reacting to it, as well as the interaction relationship between the person and the machine.

Future generations' learning habits, practices and attitudes towards education, training and learning may be very different compared to current generations, requiring both research as well as the development of training and education structures, methods and tools. The training and education system must be able to adapt to changes in society and continue to provide a motivating and effective learning experience that serves as the basis of the reservist army's capability and national defence will.

The central themes of this field of study include human performance, the human-machine interface and learning. The objective is to produce basic information and expertise related to these themes while seeking and producing new solutions.

Information operations

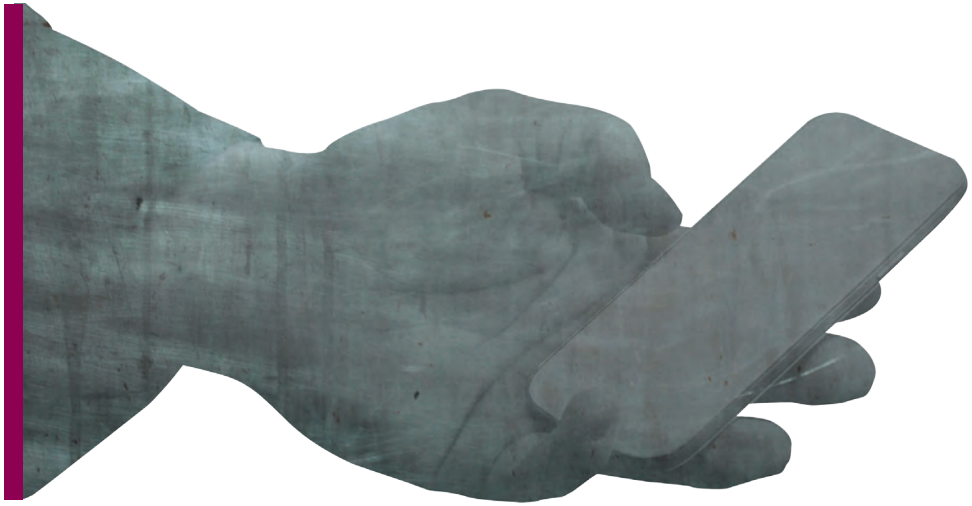
Information operations consist of methods designed to influence a country's societal and military decision-making and capability, the opinions of its citizens, as well as measures for protecting oneself from such methods. Information operations are carried out by societal, political, psychological, social, economic and military means on a strategic, operative or tactical level. They emphasise the importance of information as the subject of operations. The aim is to affect the adversary by preventing them from forming an accurate view of the situation or by steering them into making wrong decisions. If this fails, the next step is to prevent the adversary from carrying out decisions. The psychological means employed in information operations include media operations, threats and coercion, while physical means include information network operations and electronic influencing, as well as physical influencing of targets that cannot be influenced by other means.

In information operations, the Defence Forces is just one operator among many: the government's ability to carry out information operations and protect itself from their influence requires effective cooperation between authorities and the parties responsible for societal infrastructure, as well as the media and other forms of communication that influence the opinion environment.

The methods utilised as part of information operations include intelligence, monitoring and influencing carried out in information networks; electronic intelligence and monitoring as well as electronic interference and the incapacitation of electronics carried out through the electromagnetic spectrum; and psychological and physical influence especially on the adversary's intelligence, monitoring and command systems. Means of protecting one's own operations from counterintelligence and monitoring include maintaining operational security and deceiving the adversary.

The aim of information operations is to achieve information superiority, meaning a more up-to-date and accurate situational awareness than the adversary. This is achieved by supporting information gathering, analysis and sharing, and by weakening the adversary's information processes.

The objective of the research is to create expertise and basic information related to the entire field of information operations by studying both information and people as the target, producer and handler of information, as well as means of influencing information and protecting oneself from its effects.



Networking

The development of information technology has made it possible to produce various services from locations other than the ones where they are used. In effect, functions can be distributed for use via information networks. As a result, networks provide access to a wide variety of services, even ones that you might not have known to exist. The development of networking has a major impact on civilian business models as well as the building of defence systems and the deployment of capabilities.

The networking of sensor, weapons and command systems facilitates the forming of comprehensive situational awareness and diversifies the possibilities related to the use of force. Shared sensor and weapons systems can be used to carry out centrally coordinated operations combining the resources of several branches of defence, which can be commanded from any existing command centre. Situational awareness, decision-making and use of force are not bound to any one place.

The more accurate and up to date situational awareness created by the network enables the use of mission tactics. On the other hand, a more comprehensive and accurate situational awareness, which also changes more rapidly due to the real-time requirements of the data, sets new demands for mental performance. Utilising the full potential of networking requires the utilisation of the capabilities made possible by it in tactics and command, as well as the organisation and use of systems and troops. This may also have an impact on the tasks and structures of defence and military branches.

A key characteristic of a network-centric operating method is that the service provider is present virtually instead of physically. For example, a sensor producing situational awareness operates remotely and is not personally operated. Similarly, a weapon supporting combat may not be within visual range, even though its capability is utilised through requests sent via the network. A leader does not need to be physically present, but may still assign tasks through the network. Similarly a doctor examining and treating the wounded may be present only virtually. These kinds of scenarios set special requirements for the reliability of the network and for building trust. In addition to understanding a physical data terminal, the user must also understand the operating principle of the network and have trust in it. It is clear that a network-based operating environment also adds new capabilities related to soldiers' and leaders' mental requirements.

The rapid development of mass-market information technology has created new kinds of networked business models. In addition to this, it has changed people's operating methods, as is

evident by the explosive growth of social media. However, the true potential of networking lies in the completely new operating methods and logic for building capabilities made possible by it.

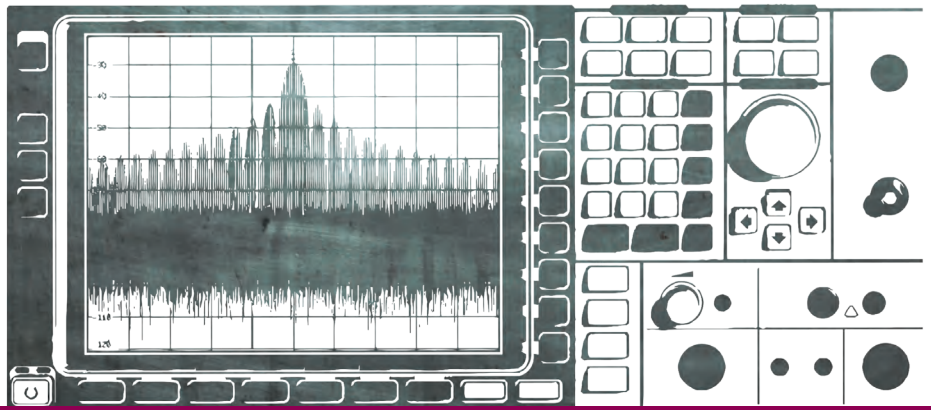
Networking is based on two technological phenomena: the trend of systems becoming software-based and the development of data transfer technology. When systems become primarily software-based, the observations, measurements and other data gathered by different devices can be transmitted electronically almost anywhere. This also means that devices can be remotely controlled using information. Data transfer technology is the glue that connects the different parts of the network together.

The capabilities of information systems are becoming increasingly dependent on the software running on them. However, as systems become increasingly software-based, they also become vulnerable to attacks carried out over the network. At the same time, more and more devices are being connected to the network, which presents new kinds of opportunities and threats. One example of this is the significantly increased potential of open source intelligence. However, at the same time ensuring the operational security of one's own operations becomes increasingly difficult.

Even though civilian technology leads technical development in the field of networking, it is clear that not all of its applications are suitable for military use as is or at all. The application of civilian technology is limited by numerous factors, such as the power supply requirements of portable devices, the upholding of operational security and securing the confidentiality, integrity and availability of information. In military environments, one must consider not only unintentional interference, but also intentional interference, the adversary's intelligence capabilities and the physical and electronic attacks directed at systems by the adversary.

Networking provides access to nearly all information. Automated mass-scale information management and data mining (big data) provides improved situational awareness and improved preparedness for changing situations.

Acknowledging the fact that the civilian sector drives development, the defence sector must first and foremost develop its ability to study, understand and apply various new technologies. Doing so also involves considering the impact that new technologies have on deployment principles and the operation of the personnel.



Capability in the electromagnetic spectrum

In manoeuvre warfare, the gathering and transfer of information is based on the use of the electromagnetic spectrum, extending from radio frequencies to the wavelengths of visible light and ultraviolet radiation. The expansion of the range of methods available in warfare from the traditional land, sea and air domains to space and information networks introduces both challenges and means related to controlling the electromagnetic spectrum. Space, for example, provides the opportunity for invisible monitoring and information transfer in a way that may have both technological and psychological impacts. Additionally, information networks can be affected by means of electromagnetic radiation. As such, fulfilling the requirements of manoeuvre warfare and networked operation requires new ways of managing frequencies in the congested spectrum.

The reduced size and increased accuracy of radar imaging technology and the development of laser-, multi- and hyperspectral imaging technologies necessitate improvements in the stealth technologies and camouflage used by troops. Means for answering the developing threat of sensor technologies include the development of counter-sensor technologies and the deployment of new material and structural technologies.

In addition to electronic influencing, protection and support, electromagnetic spectrum management involves frequency management. In future international operations, which will most likely consist of coalition-based operations, frequency management will be limited by legislation and various regulations. Because of this, frequency management requires widespread cooperation with the authorities both nationally and internationally.

Electromagnetic radiation can affect people both physiologically and psychologically. The direct physiological effects of electromagnetic radiation are already well-known based on directed energy weapons, but longer-acting phenomena require further study. However, studying the psychological effects of electromagnetic radiation is challenging since an invisible threat from space, for example, or in the form of loitering weapons is a concept that is difficult to manage, which nevertheless has an impact on troop functionality.

The increasing networking and complexity of warfare ensure that in the future the utilisation potential of the electromagnetic spectrum and the threats caused by its use cannot be evaluated based solely on individual technical systems. In addition to system functionality, such evaluations must also encompass human activity, troop deployment principles and the overall networked battlefield, including the signature background consisting of the terrain, vegetation, buildings and other targets.

Systems with autonomous characteristics

The development of information, sensor and electronics technologies will result in increasingly intelligent machines with higher situational awareness. At the same time, deeper insights into the animal world and human cognition enables us to supplement current vehicle-based unmanned systems with new kinds of distributed solutions. It is also worth noting that as machines develop, the environment is also becoming smarter. Autonomous systems can be detected, recognised and provided with information and services by intelligent infrastructures in their area of operation. These networks composed of different autonomous systems and smart infrastructure may have entirely new kinds of applications that allow totally new capability concepts.

Humans will be replaced with machines especially in high-risk tasks such as reconnaissance and operations carried out under fire. Due to the fact that machines never get tired, they are also ideal for long-term monitoring and surveillance tasks. It is worth noting that systems with autonomous characteristics are present in all operating environments: on land, sea and air, as well as the information space. Autonomous concepts are not limited only to the physical world.

Removing the need to have an operator inside the machine enables us to design smaller and lighter platforms and extend their operating time and range. When system requirements do not have to conform to human limitations, many completely new properties can be realized. Removing the various life-supporting systems also brings cost savings and enables lighter, faster and more agile solutions.

Machines are, however, not expected to become completely autonomous. The principles of international law, arms control agreements and state agreements related to humanitarian law and arms control require a human being to participate in at least some part of a machine's decision-making process. This may limit the utilisation of the machines' capabilities, at least for countries that adhere to international law.

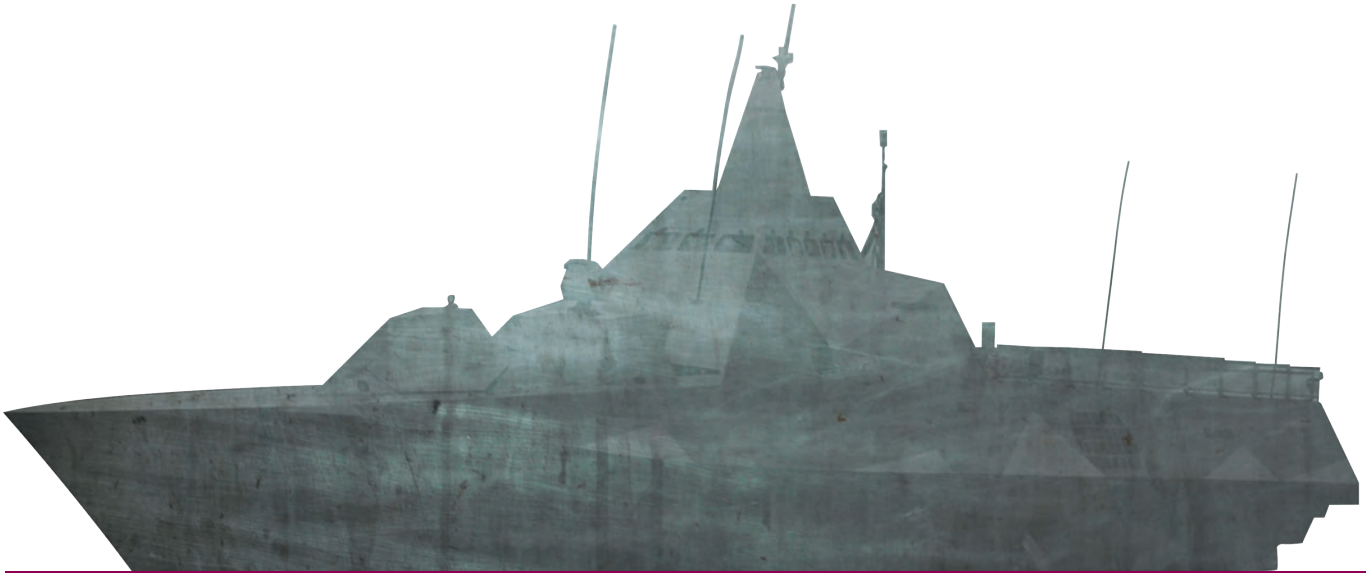
Humans are always involved in mission planning and monitoring and controlling the mission execution. Humans are also needed in arming, replenishing, maintaining and repairing machines. However, the role of the human is set to undergo a significant change. At first, humans will go from directly controlling parts of machines, such as ailerons, rudders and wheels, to simply defining routes for them. The machine then flies, sails or drives that route, automatically avoiding threats and obstacles while the human observer focuses on the environment and fulfilling the mission. As the cognitive capabilities of machines develop further, they will be given more situational decision-making responsibilities while humans focus on higher level planning. For example, a machine could be tasked with finding a specific target, after which the machine would itself determine the target's potential location and the best way of looking for it.

Machines have the ability to communicate with both humans and other machines. As a result, the role of the human will no longer be that of a machine operator, but rather that of a leader, who may be in charge of a unit comprising both machines and humans. Machines will also be capable of shared decision-making. This makes them capable of employing swarming tactics; a group of machines can, for example, jointly determine how to group up in order to defend a target based on a detected threat.

In the future, humans will not so much use machines as work together with them. These changes in the roles of machines and humans may have a significant impact on group dynamics and troop cohesion. Building trust between humans and machines requires us to not only understand people, but also be sure of the machines' reliability and intentions and develop their communication capabilities for this purpose.

As technology becomes ever smaller and cheaper, precision engagement capabilities will spread to new systems. Loitering weapons, small self-sacrificing robots that swarm and home in on their targets, small ubiquitous sensors, systems operating under hostile fire and other applications made possible by technological development introduce new ways of carrying out battlespace monitoring, target acquisition, engagement, protection and logistics. On the other hand, when used by the adversary these new technologies also introduce new threats, resulting in the need to develop new protective and countering measures.

Most safety concerns related to warfare, such as qualifications and safety regulations, are based on the assumption that they apply to humans and units consisting of humans only. Because of this, deploying unmanned systems requires the development of numerous new regulations. As autonomous systems grow more common, we will need to determine the allowable level of autonomy in land, sea and information environments as well. Doing so will require us to consider numerous perspectives in addition to national and international legislation, such as safety, authorisations and the performance of armed forces. For example, we will need to define the judicial responsibilities of the machine designer, the manufacturer, the programmer, the person planning the mission and the end user. In addition to this, moral and ethical questions must also be solved.



Implementation

The research agenda will be implemented in numerous ways, such as in the form of the Defence Forces' multi-year research programmes, individual studies as well as national and international research cooperation. The Defence Forces' research programmes (PVTO) are multi-year, target-oriented research projects, in which research and development is primarily carried out by the industry and academia. Conversely, individual studies typically consist of well-defined one-off research tasks lasting one to two years.

The research agenda describes the research themes that the Defence Forces considers to be the most crucial over the course of the next 15 years. The research agenda is maintained in accordance with the strategic planning schedule, with reviews carried out every four years.

Puolustusvoimat
The Finnish Defence Forces