OUTLOOK

Research Plan part 1

2019–2022

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment

PREFACE

Internationally, we are witnessing a changing defence and security policy landscape, increasingly complex security challenges and far-reaching technological advances. The Norwegian Defence Research Establishment's (FFI) research plan for 2019–2022 is our research response to these challenges. In part 1, "Outlook", we provide a concise and overarching view of some of the development aspects and challenges we consider most significant for the defence sector.

Research efforts must be prioritised sensibly and cost-effectively. FFI will concentrate on essential duties that others will find difficult to resolve, and where the institute can make important contributions. This requires scientific knowledge, technological expertise and professional military judgement.

Through its own research and extensive collaboration with national and international research communities, FFI is at the cutting edge of the scientific, technological and military technology developments. The consequences for the defence sector have been assessed, and we direct particular attention to emerging technologies that can create fundamental changes and make a significant difference. This insight is the knowledge base for the professional advice FFI provides to the Armed Forces' political and military administration.

This is also the basis for FFI's contribution to industrial and technological development in Norway. Within the frameworks of FFI's mission and the guidelines in the national strategy for the defence industry, we undertake assignments for civil authorities, industry and businesses.

FFI is structured around projects and external funding for assignments. We assume that the level of ambition for R&D will continue at the current level and that the balance between long-term research and contract research will be maintained from 2019 to 2022.

The research plan is anchored in the Long Term Plan for the Norwegian Armed Forces and prepared in close collaboration with our most important contracting authorities, both within and outside the defence sector. I hope this provides insight into some of the global development aspects that have the greatest significance for the defence sector, and that it also provides a better understanding of the prioritisations that will guide the defence sector's R&D in the coming planning period.

John-Mikal Størdal
Director General

Internationally, we are witnessing a changing defence and security policy landscape, increasingly complex security challenges and far-reaching technological advances.

INNHOLD

Technological trends — what do they mean for the Armed Forces?

Science and technology have created, are creating and will continue to create fundamental changes. The introduction of aircraft, nuclear weapons, missile technology and precision-guided weapons have all resulted in entirely new operational concepts. It is especially important to be aware of technologies that may have such consequences. In our time, the developments within electronics and information and communications technology (ICT) are considered to have such a potential.

In other areas, the development is more gradual. These are advances that do not result in fundamental changes in the short-term, but which in sum and over time may nevertheless have major consequences. This also requires attention, since such trends may have a tendency to go undetected and can pose challenges if they are not put on the agenda in time.

There are many historical examples of retaining military systems long after they have become outdated. For instance, battleships were part of the USA's force structure until 2006, despite the fact that far less expensive and more impactful missile platforms were available.

One of FFI's most important duties is to keep abreast of aspects of technological developments that may impact the conditions for the defence planning. Below, we will highlight some of the most important development aspects and the potential consequences for the Armed Forces, both in the short and long term.

Technological hegemony is weakened

The 1991 Gulf War revealed an enormous gap between American capabilities and that which states such as China and Russia could have assembled at the time. This gap is now considerably smaller.

The USA remains on top in terms of defence-related research and development (R&D), and allocates more than 50 percent of its public R&D investments to military R&D. The U.S. military's R&D budget was NOK 500 billion in 2017. This represented twelve percent of the total defence budget. The EU has initiated programmes to strengthen its own efforts in this area, but still appears modest in comparison to the USA.

China and Russia have increased their defence spending considerably, with major efforts also in the area of R&D. Since 2008, Russia's defence modernisation has provided the country with capabilities previously solely held by Western states, and China's immense economic growth has resulted in a similar development. Meanwhile, there have also been advances in the West, although this has not prevented the gap from narrowing. For instance, the much-discussed "Third Offset Strategy" has not produced any revolutions in the way in which the Americans operate.

It is now the civil sector that spends the most on technological development, in contrast to the Cold War period. The company Apple, for instance, invests more in R&D than the entire Norwegian defence budget. Areas such as autonomy and artificial intelligence are first and foremost driven by the fact that they have a great commercial potential. Such technologies will also affect the military domain, and the rapid pace in the civil development is challenging the relatively protracted military procurement processes. At the same time, much of the civil R&D activities are short-term and commercial, and often build on the more fundamental efforts aimed at military needs. These are not mutually exclusive, and it is important to quickly put civil technology to use wherever this is relevant.

Trends

Trend analyses in recent years by various research communities show a consensus on which technological areas will have a major and increasing importance for military operations in the future. Areas that stand out include artificial intelligence, additive manufacturing, quantum computing, nanotechnology, the Internet of Things and autonomy.

Consequences for operational capability

The motto "strategically defensive – tactically offensive" was used during the most recent Strategic Military Review (fagmilitære råd (FMR)). In the Land Power Study and the subsequent recommendations, this was followed-up with a greater emphasis on long-range precision-guided weapons. Our military must also be viewed in an alliance context. For instance, we must be capable of operating seamlessly with the Americans in what they refer to as "multi-domain battle". The procurement of F-35 also indicates a shift in the existing defence concept. The capability to affect an enemy in more ways than passively defending a line is becoming more important, but new technologies are a prerequisite for being able to realise a more offensive mode of action. Much of this technology is already available. The challenge for the Armed Forces is to facilitate a more systematic introduction of these technologies.

In order for the three technology fields sensors, communication and weapons, discussed in the fact box on the right, to be able to work together, we are also dependent on an effective command and control system (K2).

Some important technology fields that stand out

1 **SENSORS**

New technology such as hyperspectral sensors can provide us with entirely new capabilities and make it very difficult for enemies to camouflage themselves. We must invest in new sensor platforms, but the optimal mix of human intelligence, UAVs, AUVs, satellites and manned platforms has yet to be determined.

2 **COMMUNICATION**

The current communication systems are insufficient and vulnerable when assessed against future requirements for operational tempo, collaboration and geographical coverage. This applies to all areas: strategic, joint operational and tactically. High-frequency communications systems are becoming significantly cheaper and available on the mass market. Higher frequencies for communication improve the transmission capacity, and can also reduce the possibilities of both interference and jamming. Furthermore, investment is needed in communication platforms that provide redundancy. This may involve larger and smaller drones and satellites, but also the capability to use available networks ad hoc – e.g. commercial mobile networks.

3 **WEAPONS**

We require a broad spectrum of different types of weapons that can deliver at somewhat greater distances and with great precision – in order to destroy the target, and also to minimise unintended harm. Currently, we have NSM and are in the process of developing JSM, but these can only be used for high-value targets. Stealth technology and planned arms for F-35 will also result in a marked improvement of the Armed Forces' capabilities, but there may also be a need to develop or procure new types of weapons.

◂ When technological advances in different fields work together and reinforce one another, it can fundamentally change future operations.

> Given that adversaries can now impact us physically, with long-range precision-guided weapons, and also in cyber-space, with short or no notice, how can we ensure the capability to receive and communicate decisions at all levels?

Here, technological development presents new possibilities, but also challenges: Given that adversaries can now impact us physically, with long-range precision-guided weapons, and also in cyberspace, with short or no notice, how can we ensure the capability to receive and communicate decisions at all levels? NATO has defined cyberspace as an area on level with land, sea and air. What does this mean for us? Perhaps we need to completely re-think the K2 field, in terms of both concept and structure.

Efficiency improvement

The ability to utilise new technology will be crucial also in peacetime and in smaller crises. In the civil sector, we are seeing companies that are improving efficiency through automation and robotics – in very different areas. For instance, artificial intelligence may replace trainee lawyers in mapping legal source materials. Will the Armed Forces be capable of utilising such technology to improve the efficiency of logistics, administration and operational activities?

The total defence

Technology that was previously only available to nation states, is now increasingly being spread to non-state actors and individuals. This presents society with new challenges. Here we can mention threats in cyberspace, chemical and biological weapons, small drones with explosives and much more. To be able to meet such challenges, we must not only have an effective military defence, but also a good cross-sectoral cooperation – i.e. an effective total defence.

Convergence

An important aspect of the technological development is convergence. When technological advances in different fields work together and reinforce one another, it can fundamentally change future operations.

New sensor technology, combined with autonomous swarms of unmanned systems and artificial intelligence will, for instance, be able to provide an actor will near real-time situation awareness in a future theatre of operations. An enemy who lacks this, or who is incapable of preventing its enemy from acquiring this, will be completely inferior. Here it is worth noting that such visions of the future have been discussed – and exaggerated – for many years. Paradoxically, concepts such as "network-centric warfare" have almost become outdated, precisely at a time when technology has reached a stage where many of the underlying ideas can be realised on the battlefield.

Primary challenges of the Armed Forces

The Long Term Plan "Capable and Sustainable" emphasises increased military readiness and strengthened defence capabilities. The background for the prioritisations involves a more challenging security situation in Norway's immediate regions and the recognition that the current infrastructure is underfunded.

Security policy challenges

A gradual power shift from the West to the emerging major powers in Asia and parts of Latin America is currently taking place. At the same time, new actors are gaining greater political influence, both globally and locally. Overall, the development is moving in the direction of a world where power is distributed more evenly between more state and non-state actors. Persistent disagreements between major powers may, in the worst case, challenge the current international legal system, which is Norway's first line of defence.

Russia continues to be our greatest security policy challenge. In recent years, Russia has strengthened both its military capabilities and the capability to coordinate the use of military and non-military means. Military use of force, particularly in the Ukraine, has been accompanied by extensive use of other means of influence – propaganda, cyber operations, economic pressure and international diplomacy. Russia's military capability to establish denial in Norway's immediate region is a relevant problem in light of their presumed need to protect the Northern Fleet's nuclear submarines. Russia has also implemented new systems for electronic warfare, long-range land and sea-based air defence and precision-guided weapons for use against air, sea and land targets.

In the years to come, Russia will remain a major power with the capability and intent to use military force regionally. It is anticipated that the country will maintain an aggressive foreign policy in relation to the West, although it is uncertain how long it will have the economic capacity to do so. At the same time, we can expect comprehensive economic and political reforms. Defence modernisation continues, but not necessarily at the same pace as in recent years. Nevertheless, we expect that the Armed Forces will be highly prioritised. The greatest uncertainty relates to the domestic political development after Putin's last term.

The greatest threat to Norway would be if Russia continues its authoritarian development and considers military force to be its most important foreign policy tool. Norway may be subjected to various forms of military pressure, likely in combination with other means of influence. This may occur on short notice.
NATO continues to be Norway's guarantor for allied assistance, but the collective will and capability to defend us may become more uncertain. This is partly due to demographic trends in Europe, China's growth in other regions and domestic policy developments among allies. Bilateral relations and greater defence and security policy collaboration with more states can therefore be an important supplement for Norway. The USA remains our most important ally, but this support depends on what the USA itself wants, as well as developments in other parts of the world. Overall, global trends indicate that Norway must expect to take greater responsibility for its own security, because the prospects of allied support may become more uncertain.

Increased investment in the Armed Forces

Since the current Long Term Plan was presented in 2016, the government has followed up with increased investment in the Armed Forces. Several of the demonstrated gaps in surveillance and control of the air space will in the near future be filled by new air surveillance radars and strengthened air defence capabilities. Furthermore, readiness has been improved by, among other things, more days at sea and more training. NATO's two percent target from 2014 has resulted in additional political parties calling for an increased investment in the Armed Forces. However, it remains to be seen how this will be reflected in future defence budgets and how such an increase will generate increased operational capability.

Even with a development heading in the right direction, a few challenges still remain. A sound defence structure has a real balance between duties, structure and finances. This is the foundation for the Long Term Plan. It means that there must be coherence between the role and the duties the Armed Forces have, and how the defence structure will be developed. This requires a comprehensive, conceptual understanding of how all capabilities of the Armed Forces should be utilised. Persistent underfunding will reinforce an already dramatic deficit. At the same time, it limits the scope of action for implementing new technology and managing continuous innovation. A good balance between investments in new materiel and the opportunity to operate sufficient training and exercises must be secured. The latter is important for safeguarding the requirement for readiness. This will be one of the main challenges for the Armed Forces in the future, and it will be necessary to find smarter ways of operating training and exercises. It is also important to consider the specific cost increase for the Armed Forces.

The military land force challenge

Norway has unique challenges in terms of securing sufficient response capabilities and endurance. Large areas of land with considerable distances requires especially well-functioning supply chains. For a military land force operation, this will greatly

New capabilities and the use of these will also influence the Armed Forces' method of operations. New combat aircraft, submarines and missiles will not only influence doctrines and tactics, but also our perspectives on defence. In light of new threats and in close collaboration with the military branches, FFI has initiated the process of identifying and simulating the operational consequences this will have.

influence military capabilities. It is therefore crucial to maintain a good balance between active presence and the capability to pose a threat at greater distances. This applies both to materiel and the capability to deploy operationally-ready personnel with sufficient training for the mission.

Some challenges therefore remain for the continued development of land power. The 2017 Land Power Study recommends strengthened presence in Finnmark, with, among other things, the establishment of the Finnmark army command and the restitution of a separate squadron. Collaboration between the Army and the Home Guard will enhance readiness, and coordination of training, equipment and plans for the active reserve will result in strengthened military land force capabilities in this part of the country. However, there are also challenges associated with the defence of the rest of the country. This especially applies to the role of the Home Guard as part of the land power and what is required in terms of personnel and equipment to fill this role.

Intersectoral collaboration

The Home Guard also has an important role in asset protection. In collaboration with civil authorities, this is also an important task for the Armed Forces. New technology should to a greater extent be put to use for surveilling assets, processing information about them and actively inspecting them. Sufficient protective security measures for the Armed Forces' sensitive assets must be ensured through measures and systems that can respond to a wide range of threats. Several of these threats will be unpredictable. The approach to this topic must therefore correspond with the manner in which large-scale threats are treated.

New types of threats

There are also other types of influences, for instance, cyber and information operations and threats from international terrorist networks. The development of the entire Armed Forces must be viewed in light of this new threat landscape, and it is necessary to define a defence structure that can cover a broader spectrum of conflict. In this context, it will be important to further develop civil-military cooperation and strengthen the capability to handle threats that challenge the boundaries between the defence and justice sectors.

Personnel and competence

With respect to personnel, several important changes have been implemented in recent years, including a new personnel structure, introduction of general conscription and a new education reform. It is anticipated that this will result in the Armed Forces becoming better at recruiting and retaining personnel. However, challenges still remain regarding the appropriate administration of conscripted personnel and challenges with ensuring sufficient diversity within the organisation.

New technology and the introduction of new capabilities will influence the Armed Forces' need for expertise. It will be important to identify the duties that will disappear and the new competence needs that will arise, as well as the challenges related to the interaction between people and new technology.

New operation methods

New capabilities and the use of these will also influence the Armed Forces' method of operations. New combat aircraft, submarines and missiles will not only influence doctrines and tactics, but also our perspectives on defence. In light of new threats and in close collaboration with the military branches, FFI has initiated the process of identifying and simulating the operational consequences this will have.

Capable and Sustainable

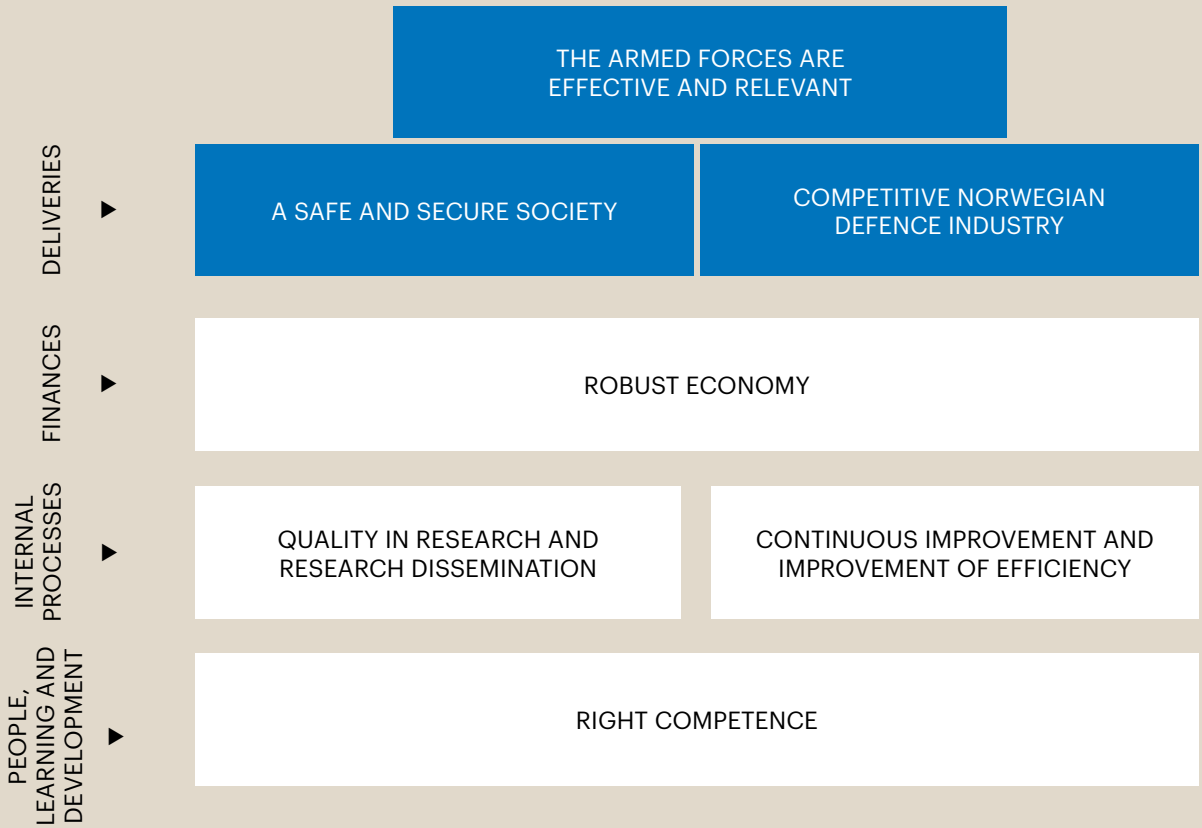
There is broad political agreement for strengthening defence capabilities in order to deal with the new security situation. Contrary to past situations, there are signs indicating that this will is backed up by action. The four important principles for continued development of the Armed Forces are firmly established. Firstly, this is a true balance between duties, structure and finance, and secondly the development of the Armed Forces should take place within a comprehensive framework. This entails that the Armed Forces should function as a system comprised of several sub-systems. The interdependence of the various structural elements is partly understood and considered in the new operational concepts. However, there is still considerable room for innovation. This will require a holistic approach that extends beyond the current planning period. The basic structural components of the Armed Forces are combat aircraft, surveillance capabilities and naval and military land force control. There are also operations in cyberspace and utilisation of this space. Unpredictable future defence budgets will be a challenge in this process, but a process that is able to identify opportunities and consequences of political choices must nevertheless be facilitated.

Understanding the technological opportunity space

The latter two principles – regarding increased realism in the defence plans and that decisions must be viewed in a long-term perspective – are likely the most crucial, but also the most challenging. Short-term sub-optimisation occurs at the expense of structural changes that require time and targeted adaptation to a new reality. This applies not least to the technological opportunity space, where there is a consensus that it is costly to put new technology to use. This is also correct, in many contexts. At the same time, new technology is entirely necessary for the Armed Forces to be relevant and have a real deterrent effect. However, this is just as much a matter of insight into the technological development and knowing what it entails in the short and long term. This is the main objective of all evidence-based research being conducted, whether at FFI or other expert communities in the defence sector. The time when a select few had a monopoly on this knowledge is over. The open information society has made knowledge more easily available. The current challenge is to be able to utilise it and place it in a military-operational context. There are still important directional decisions for the Armed Forces, and FFI aims to support the continued process with good analyses and estimations in the future as well.

On the following pages, we will provide a concise and overarching description of the most important fields of technology that form the basis for FFI's research plan and explain how the Armed Forces can utilise these. ▶

FFI'S GOALS 2019–2022



VALUES

Creative, enterprising, broad-minded and responsible

VISION

FFI turns knowledge and ideas into an effective defence

Defence planning

Defence planning is a highly complex area that affects the facilitation of the Armed Forces' capabilities and effectiveness in the future. The purpose of such planning is to ensure that Norway has the necessary forces, infrastructure capacity, capabilities and facilities to fulfil the assigned duties across the entire spectrum of missions – from missions in peacetime, crises and, in extreme circumstances, war. Long-term planning adds an extra dimension to the defence planning since it is very difficult to predict what challenges we will face in the future. At the same time, the technological development contributes to somewhat unpredictable advances that can benefit the defence planning, but also present significant challenges. This is a challenging process both for planners and decision makers.

Contexts

As previously mentioned, the main purpose of defence planning is to create a balance between the Armed Forces' duties, operational capabilities, structure and finances. A sound plan ensures that the Armed Forces' structure is sufficient to solve the assigned duties, and that the financial basis is strong enough for the structure to be realised, both from a short-term and long-term perspective. The Storting (Norwegian parliament) determines duties and level of ambition, and the planner's job is to adapt structure and finances so that the duties can be solved in a cost-effective manner, while at the same time optimising the operational effectiveness.

FFI supports the Armed Forces' long-term planning through projects and activities that assess and analyse duties, operational capabilities, structure and finances. An interdisciplinary approach with close collaboration between researchers, military professionals, specialists and political authorities is useful and has a binding effect. In the research plan, we have arranged for studies on global trends, terrorism, Russian defence development and international operations. This way we can establish a solid foundation for assessing the duties of the Armed Forces.

Scenarios

Through scenario development, security policy challenges are operationalised in concrete, analysable situations in a Norwegian context. Scenario preparations can in many ways be compared with drawing a security policy challenge map of Norway. We will approach the problem in two stages: The first stage consists of developing largely generic scenarios – scenario categories – which combined represent a categorisation of the entire security policy sample space. The second stage consists of moving in and out of each individual scenario category and preparing one of more concrete scenarios with much more specified parameters. With the aid of war games, simulations and studies of various military functions, we will map how the Armed Forces as a whole can best solve the challenges. We will design alternative defence strategies and compare these in terms of effectiveness and costs in a 20-year perspective. Through projects for strategic cost analyses, we provide a sober and realistic overview of costs and establish new knowledge regarding how the defence-specific cost increase can be handled appropriately.

Radical alternatives

FFI has a special responsibility to contribute with good, innovative solutions for the continued development of the Armed Forces. In a more long-term perspective, we will conduct studies of radical alternatives to the current defence concept. The purpose is to explore how the Armed Forces can be developed differently from the current situation. These studies contribute towards strengthening FFI's capacity to provide strategic advice to the defence administration.

In order for the approach to be as comprehensive as possible, FFI's analyses occur within a framework where the ability to prioritise across sectors and capacities is key. In a system with strong sectoral interests, these analyses are intended to offer a professionally solid, research-based and objective basis for decisions regarding the continued development of the Armed Forces.

Innovation and industrial development

Norway is a small country with limited resources and funds for its own military forces and for developing technology and materiel. NATO is an important mainstay in Norwegian defence and security policy. Defence and emergency preparedness capabilities are not solely defined by operational forces and materiel, but also by the total competence and capacity in the country. A competitive defence industry and knowledge base is an important part of our national defence capabilities.

Burden-sharing and balance between national defence capabilities and allied support is also reflected in the Armed Forces' investment plans. Norway has chosen to invest in developing a limited amount of technology and capacities, and instead rely on purchasing fully-developed, off-the-shelf products from other countries, or to develop and procure larger capacities in cooperation with allies. This has been very important to ensure cost effectiveness in the procurements of materiel, and to ensure a division of risk and development costs for the large structural elements and defence systems.

Unique Norwegian needs

Norway also has a geopolitical significance and some geographical and climatic conditions that require specially-adapted solutions. A deliberate investment in selected technological areas of expertise therefore provides a basis for the development of national expertise, technology and industry. Over several decades, we have been able to develop an effective innovation model. Key to this model is the close collaboration between user environments in the Armed Forces, technology environments at FFI and the Norwegian defence industry. As a result of this investment, we have a defence industry that is niche-based, high-tech and internationally competitive.

Attractive collaborator

There are several reasons why it is essential to maintain this position, and to further develop the established competitive advantages. Burden sharing is not merely about the forces and military capabilities we contribute to NATO operations or other international operations. It also involves the ways in which we contribute to developing cost-effective collective defence capabilities. By possessing special expertise within our niche areas, we become an attractive collaborator in military operations, exercises and training, and within research and development and industrial cooperation.

Military research and development also contributes to a safer and more secure society through spin-off and dual use. This also contributes to increased value creation for society, along with the value creation from exports of Norwegian defence technology.

The triaxial collaboration model

The triaxial collaboration model has been an effective innovation model for the Armed Forces and has been the basis for developing new capabilities in a national framework. Some of the success criteria include user-driven innovation, long-term research and development and trust-based collaboration. It is also important to have orderly role management, a coherent range of instruments and predictable funding. At the same time, we have achieved optimal interactions between the national and international market. The model allows us to concentrate available funds and resources. In this manner, we achieve cost-effective development of solutions for the Armed Forces. The triaxial collaboration model version 1.0 has served Norway well, historically speaking. In light of ongoing development aspects, it will be necessary to further develop this innovation model.

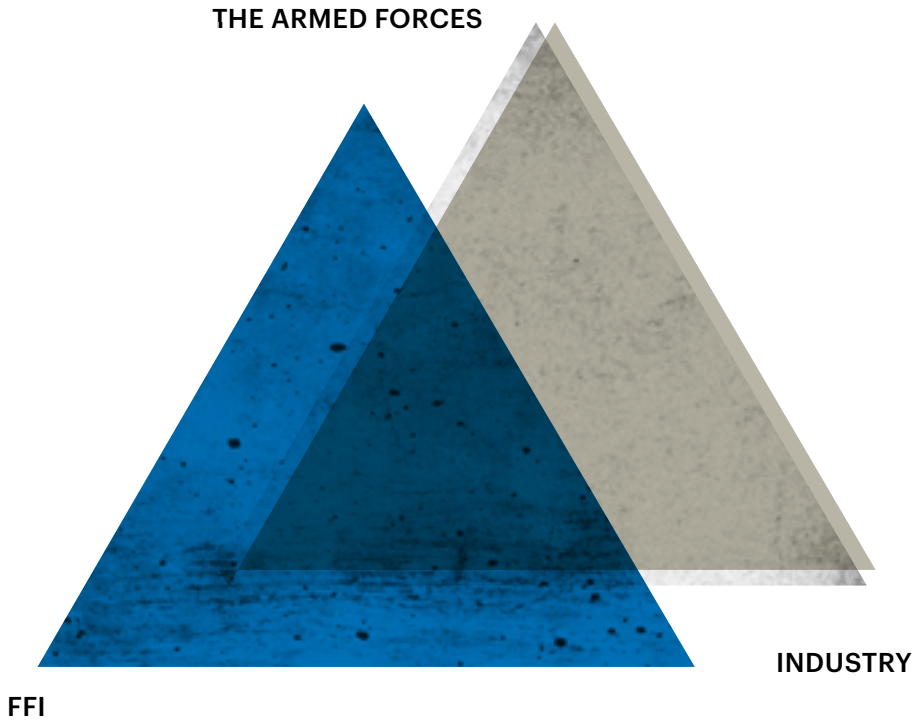
Must further develop the innovation capacity in the sector

Rapid civil technology development is one of several development aspects the Armed Forces must be capable of using to its advantage when new solutions and materiel are developed and procured in the future.

Rapid civil technology development also results in a rapidly changing threat landscape. This is especially applicable when non-state actors gain access to advanced civil technology.

NATO's investments in joint operations is another development aspect to which the Armed Forces must adapt, not least in terms of materiel. This entails major requirements for information exchange between the units, in terms of interoperability, capacity and reliability.

The organisation of European defence research and defence industry is undergoing significant changes, driven by a need to become less dependent on the USA. Here, the EU is a key actor, and Norway's role is challenging. A desired restructuring within European defence technology and industrial base is justified by the fact that Europe is lagging behind compared to the USA and Asia.



Increased national security and emergency preparedness capabilities, including strengthening of the total defence, is more heavily emphasised than before in the current Long Term Plan and Report to the Storting (White Paper) 9.

The same development aspects are the reason why our allies have initiated several new investments in defence-related innovation. A common feature of these is the intent to utilise civil and commercial technology in developing defence materiel faster and cheaper, and execute defence procurements more rapidly, and adapted to the technological development.

Need for a triaxial collaboration model version 2.0

In Norway, we must preserve the strengths of the established innovation model, but also add some extra functionality to establish a Triaxial Collaboration Model version 2.0 that can serve us well also in the future.

Some keywords for the extra functionality are:

- better use of available commercial technology
- stronger involvement of small and medium-sized industrial actors and entrepreneur communities, both civil and within the defence market
- better collaboration between civil and military R&D and technology to extract the potential of dual use
- increased mobilisation of civil expert communities that can contribute to developing solutions for new threats and new needs for the Armed Forces and the Total Defence
- facilitate arenas and networks where users, researchers and the industry collaborate to develop and experiment with existing and new technology
- early exposure of technology and solutions for user environments, as this has been shown to be an effective tool to stimulate more rapid innovation.

A new innovation centre — ICE worx

As a response to this development, FFI has established a new research division for innovation and industrial development. Among other things, the division is planning to establish ICE worx, which will become a centre for innovation, concept development and experimentation for the defence structure. This innovation centre will organise actors, tools and processes that can support rapid problem solving and develop new solutions based on utilising available commercial technology. Testing and experimentation in laboratory facilitates and in the field will be key to these activities.

Sensor and weapons development

The Armed Forces operates advanced sensor and weapons systems on a wide range of platforms including satellites, aircraft, drones, combat vehicles, artillery, frigates and submarines, in addition to permanent installations.

FFI has strong expert communities that can support such systems throughout the life-cycle, from concept phase and development to procurement and operation. For many of these systems, no one in the Armed Forces other than FFI has extensive expert knowledge. FFI also uses this expertise to support defence planning, including the assessment of potential threats.

Both large and small systems

The development of sensors and air defence systems for larger platforms means both higher performance and higher costs. New generations of long-range radars, sonars, missiles and ammunition require more testing and analyses, both during procurement and operation. Here, the Armed Forces often makes use of FFI's expert knowledge.

Commercial sensor technology is rapidly developing in the direction of small and inexpensive systems with excellent performance. Not only passive optical and infrared cameras, but also lidar and radar technology are being developed commercially, including for the automotive industry. This opens for new forms of usage for sensors in the Armed Forces, especially at the tactical and combat-technical level, and also leads to changes to the threat landscape. In the years to come, FFI will be studying sensor systems that can be integrated in soldier equipment, or that can operate unmanned, for instance, on drones, vehicles and boats. We are following this development closely and will also participate with our own research and development in selected areas. An example of innovative use of commercial sensors is the AIS satellites. Here, FFI has taken a lead in proof-of-concept studies and development.

With unmanned platforms it is also possible to make swarms of cooperating sensors that provide an entirely different functionality compared to what a single platform can offer, for instance, by synthesising a large antenna. By drawing on FFI's work on autonomous systems, new concepts for sensors based on swarms of small and inexpensive platforms will be developed.

Must keep abreast of the development

Some aspects of current technology are approaching the limits for performance, such as cameras for visible light. However, many sensor types are still far from reaching their performance limits. For instance, it is possible to utilise quantum mechanical effects to make more accurate clocks, or to develop gravimetric sensors that can map underground facilities. Micromechanics can form a basis for compact and GPS-independent navigation sensors. In the future, FFI will keep abreast of such potentially groundbreaking technology areas, in part through its own research activities.

Modern sensors produce large quantities of data. For military users, it has been an urgent problem that manual interpretation requires a great deal of time and significant personnel resources. In recent years, there has been a revolution in the field of artificial intelligence, which means that it is now possible to have machines that interpret sensor data, which previously required manual work. FFI is well-placed in this development. In the future, we will make significant efforts to ensure that the Armed Forces are able to take part in the technological development across the board.

In the context of weapons development, FFI supports both the Armed Forces and Norwegian industry in developing ammunition and conventional weapons, including missiles. Laser weapons is an area that has considerable potential. FFI has a great deal of research activity on laser technology and is closely following developments in this field. We are working with various types of seekers and propulsion systems for missiles and have particularly good expertise on passive IR seekers and solid-propellant rocket engine technology. In recent years, we have studied new technology for ramjet engines that can give missiles supersonic cruise speed over great distances. In recent years, FFI has placed considerable emphasis on research in the area of radar technology. Based on this expertise, FFI has been chosen by NASA to develop a ground penetrating radar for an unmanned vehicle which will soon be sent to Mars.

▸ Flight test of JSM at Utah Test and Training Range in the USA in March 2018. The missile avoided the decoy target and hit the actual target without human intervention (autonomously).

Artificial intelligence and big data for better decision-making bases

Where is the enemy? What is she planning to do? These questions are fundamental for military operations. Providing a good answer is a bit like searching for a needle in a haystack – we know it is there, but it is almost impossible to find. Existing and new systems have a key role. New systems include F-35 combat aircraft, satellites, P-8A maritime surveillance aircraft and drones. All these systems contribute with data, and the total quantity of data is quickly growing. More data is attained from other sources.

Data is complex

Pictures, videos, positions, text reports, radar plotting, observations, streams of positions and video, database queries and network logs are just some examples of data that may contain important information. "Big data" is often used to show that there is much more now than in the past. In order for the Armed Forces to make use of the data – for instance to achieve better situation awareness and more effective target acquisition – investments are required in automated, integrated analysis of data from many sources, and in solutions and services for data management. The total defence is also in need of improvements in image exploitation, integrated exploitation of data from multiple sources and active information retrieval.

For as long as they have existed, computers have had a key role in the analysis of data. Now, however, there has been a change of course. This change of course is driven by the exponential increase in computing power combined with breakthroughs in methods for recognising patterns in data based on training data. Terms such as "artificial intelligence" or "machine learning" are commonly used for such methods. Machine vision, language processing, voice recognition, robots and image recognition are examples where artificial intelligence has been shown to be effective.

Reciprocal effect

The relationship between big data and artificial intelligence is reciprocal. Big data increases the training basis for artificial intelligence. When there is more hay in the stack, techniques for searching for the needle must improve. Artificial intelligence is a key technology for increasing the degree of automation in many systems. In this manner, systems become more autonomous, and self-driven vehicles or crafts on land, water or in the air are examples of this.

New methods for finding the "needle"

The Armed Forces should utilise techniques from artificial intelligence to the extent possible in order to handle the volumes of data that existing and new systems generate. In combination with other sources, there is great potential for improving situation awareness and laying a foundation for better decisions. FFI will research and further develop recognised techniques that are used internationally and commercially. When combined with the unique data from the Armed Forces and adapted to military duties and needs, it will produce good results. Although there is more hay in the stack than ever before, these methods will be of assistance. Rather than poking through the entire haystack straw by straw, we can burn the hay and the needle will shine through the ashes.

Autonomy and unmanned systems

Norway has large land and sea areas and we are not a large population. This means that we must be efficient and use our resources wisely. Can technology help us with this? Can we use technology to compensate for our small population?

The performance of machines has developed enormously over the past decade. Computers assist us in a growing number of areas – in diagnostics and developing medicines, verifying our passports at the airport and searching for planets in outer space. Computing power has been developing at a faster rate in recent decades. This computing power, combined with electronics, has given us better robots. These robots are becoming a part of our daily lives. They vacuum the living room or mow the lawn. Soon our cars will be self-driving. How can computing power and robots help the Armed Forces?

An enemy wishes to make the situation complex and difficult to handle. He wants the element of surprise and to act so quickly, his adversary is unable to keep up. Here, machines can help us.

Faster

Computers are much better than humans at extracting information from large volumes of data and sorting the information according to objectives. Whoever has the informational advantage can make sound and quick decisions, even under pressure and in complex situations. In many circumstances, processor speed is crucial for survival, for instance in missile defence of our frigates. Humans are not fast enough to react appropriately in such situations. To collect data and achieve situational awareness, we must be present where things are happening. This often applies to very dangerous missions, and we have to cover large areas. We do not have sufficient manpower to do this. Here, technology can help us scale up and expand our capabilities. If the technology becomes inexpensive enough, we can have many systems. Machines can cover vast areas and notify us of what is happening, and the loss will be less significant for cheap and easily replaceable machines. The ability of machines to interpret data is also what is needed for remote controlled systems that require personnel to transition into autonomous vehicles, i.e. systems that can solve tasks on their own. Cognitively demanding routine tasks can be left to machines and humans are then free to attend to other duties. In the future, we can envision autonomous unmanned systems surveilling our territories, conducting reconnaissance before soldiers advance and locating targets with precision-guided weapons.

Effective

Precision-guided weapons are also a product of this technology. Scenarios such as in the Second World War, where a city is carpet bombed to take out a factory, are no longer relevant. Precision-guided weapons utilise computers' ability to process sensor data en route and navigates precisely to the target, identifies it and strikes the site intended by the operator. Effectiveness is the objective: A missile takes out one target, without striking anything other than what was intended.

> Precision-guided weapons utilise computers' ability to process sensor data en route and navigates precisely to the target

Great potential

Machines can relieve our minds, but they can also relieve us physically. Movements require quick and good mobility. In the civil sector, transportation tasks are crucial for the development of autonomous systems – moving people and goods from A to B. Transportation or logistics are also important for the Armed Forces. A lack of supplies can weaken capability in combat and slow movement hampers progress. Machines can perform logistics tasks and they can carry soldiers' equipment. In this way, humans can attend to other duties and save their energy.

The performance of machines has increased significantly in recent years, and continues to improve. In the coming years, it will become even more important to further explore what machines are good at doing. We must also further explore how man-machine interaction can further improve so that humans are free to perform other duties. Technology has a great potential in a small country like Norway.

Cyberspace

Similar to the rest of society, the Armed Forces is dependent on cyberspace. Not only are considerable assets exposed via cyberspace, but cyberspace and the use thereof now constitutes a significant asset per se.

This is reflected in the fact that NATO in 2016 recognised cyberspace as a domain of operations along with land, air and sea. NATO is currently preparing a separate doctrine for military operations in cyberspace, so-called cyber operations. The current Long Term Plan for the defence sector also emphasises that the capability to resist attacks in and via cyberspace is important in enabling us to defend the country. As in the other domains, it is desirable to secure freedom of action, while simultaneously denying the same to the enemy.

Intelligence and influence

The open threat assessments from the Intelligence Service, Police Security Service (Politiets sikkerhetstjeneste (PST)), and the National Security Authority (Nasjonal sikkerhetsmyndighet (NSM)) all emphasise the threats in cyberspace, in the form of sabotage, influence and, not least, intelligence. Companies in the defence sector are among those considered to be particularly vulnerable intelligence targets. In other words, the sector faces actors that may be willing to use considerable resources to achieve their targets in peacetime, crises and war. Foreign states may also attempt to influence public opinion and political processes with the aid of influence operations, for instance, through smear campaigns on social media. Cyber attacks can also be an effective component in an influence operation.

Vulnerability

The fact that an unwanted incident has not occurred does not mean that we are not vulnerable. For instance, the threat actor may not yet have had sufficient motivation or the right circumstances. Undetected information leaks or preparations for sabotage may already have weakened our defence capabilities without our knowledge. The special threat to the defence sector entails that what is probably sufficient for other organisations is not necessarily sufficient for the Armed Forces. The current Long Term Plan also identifies ICT security as a priority area. We will never be able to fully protect ourselves. ICT systems are becoming increasing complex and interconnected, which increases the likelihood of vulnerability and access to exploit it. We must nevertheless become capable of implementing the appropriate security measures, and security must be an important premise setter in digitisation. Digitisation has failed if the security risk becomes so great or the security measures become so costly that the gains, in essence, are lost. In practice, this requires that we have good preventive security, while at the same time we are able to gain an overview of unwanted incidents and handle them quickly. In an acute situation, we must be able to operate with compromised systems for a prolonged period.

Cyber security and operations

FFI is planning research activities across this problem complex. Research ranges from how to identify and design appropriate security measures, including cryptography and more effective forms of detection, to incident handling and cyber operations. Cyber operations are also considered in the context of electronic warfare and operations in other domains, and in connection with the underlying information and communication infrastructure.

The technology development also results in new opportunities and challenges for security. Autonomous systems are in strong growth, and often have special requirements for security solutions. Big data and artificial intelligence are of great use, including to detect cyber attacks and other incidents. At the same time, the use of machine learning and artificial intelligence can be vulnerable to manipulation of the results.

Civil-military cooperation

Norway is facing complex and complicated threats and risks. An important development aspect is a gradual, seamless transition between societal security and state security. Civil-military cooperation within the framework of the total defence concept is a linchpin in Norwegian emergency preparedness and crisis management. The Armed Forces and civilian society must support one another reciprocally and cooperate on preventing, planning for and managing crises. FFI's research must contribute to improved civil-military cooperation.

FFI's research on terrorism and asymmetric warfare is leading nationally and very highly regarded internationally. The objective of the terrorism research is to provide Norwegian authorities with better situation awareness in an increasingly fragmented threat landscape. Conflicts in Europe's immediate regions may provide conditions for violent extremism and growth in trans-national terrorism. Terrorism research is intended to provide knowledge on non-state actors with links to states in the belt from Mali in the west to Afghanistan in the east. This will provide a better decision-making basis for political authorities, the Armed Forces, the police and civilian society generally, so that they can plan for this threat.

Civil-military cooperation

In order for the Armed Forces to be able to defend Norway's security and sovereignty in a national security crisis or armed conflict, they are completely dependent on support from civilian actors, both public and private. The Armed Forces require fuel, food and water, and need support for transportation, health services, electronic communication services and power supply. When societal security is threatened by natural disasters, major accidents or terrorist attacks and sabotage across the entire spectrum of crises, the Armed Forces' assistance in crisis management is important. It is often crucial. The current Long Term Plan for the defence sector and the Report to the Storting on societal security emphasise a need to further develop the total defence. This is now being followed up in the development of the emergency preparedness system, in underlying plans, in civil-military cooperation concepts and in intersectoral exercises. It is important that this development continues and is reflected in the subsequent long term plans for the defence sector and in the plans of civil authorities.

The total defence

FFI will contribute with knowledge, identify opportunities and give recommendations that will further develop the total defence. This work will be based on comprehensive analyses and interdisciplinary research. This involves cooperation between the research programme Protection of Society (Beskyttelse av samfunnet (BAS)) and technology research programmes on, for instance, cybersecurity, space research and autonomous systems, in addition to the support for the long-term planning. The objective is to assess whether the implemented measures and arrangements within the total defence are appropriate and forward-looking in light of changes occurring in society. An important development aspect is that private actors are responsible for a growing number of inputs for military and civil crisis management. A linchpin in such a future will be methods for developing and administering knowledge, in addition to the ability to communicate complex matters between very different types of actors.

New vulnerabilities

Public electronic communication services (ecom) are crucial for effective emergency preparedness and crisis management. Here, the Armed Forces and civil actors are very dependent on one another. In this field, the technological development is occurring rapidly and with considerable pace of change. Virtualisation technology, semantic technology, new protocols developed outside the traditional telecommunications industry and the use of cloud-based services will over time be incorporated into all forms of network functions and services. Within a short period of time, new systems with completely new and unknown vulnerabilities will be put to use. Good insight into how this development will affect all actors in the total defence is necessary. FFI will explore methods for understanding vulnerability in modern electronic communication services and how it affects risk, and assess whether it is appropriate to develop new robust services specifically targeting the Armed Forces and the total defence.

Chemical and biological weapons

The effects of chemical and biological threat agents and weapons can have widespread consequences for the Armed Forces and the rest of society. In extreme circumstances it can lead to the loss of lives.

The events in the USA (2001), Moscow (2002), Syria (2013-), Kuala Lumpur (2017) and the UK (2018) indicate that the threat of chemical and biological weapons is real and on the rise.

Development of groundbreaking technology

There is a rapid development of groundbreaking technologies than can affect the risk of chemical and biological weapons, including within chemical engineering, nanotechnology, synthetic biology and neuropharmacology. At the same time, we are seeing that information technologies, digitisation and computational methods are increasingly utilised in chemistry and biology. Most of these technologies will be useful for society. However, there is a risk that these technologies can be abused or have multi-purpose potential. In this context, we often refer to an approach between chemistry and biology as research fields. We are now seeing bulk and fine chemicals produced with the aid of biological processes. At the same time, chemical and biotechnological methods for changing microorganisms are being utilised, which can lead to a change in the virulence of the organism. This will present new challenges in addition to the threat posed by traditional chemical and biological weapons. FFI will therefore monitor these developments closely to consider whether the technologies pose a security challenge, and whether they contravene applicable disarmament conventions or impact the Armed Forces' defence against chemical and biological threat agents and weapons.

Scientific long-term study under the direction of NATO

The threat posed by chemical and biological weapons is also affected by changes in the global security policy, geopolitical and military situation. NATO has therefore initiated a scientific long-term study to identify capabilities gaps related to defence against chemical, biological and radiological weapons. FFI is heading this study, and the objective is to provide a knowledge base for strategic decisions. The recommendations from the study will be followed up in FFI's future research projects.

CBRNE emergency preparedness

The defence sector's Long Term Plan "Capable and Sustainable" has determined that the efforts to improve the Armed Forces' CBRNE emergency preparedness should be continued. Furthermore, the Long Term Plan notes that the defence sector will further develop the capabilities to assist civil authorities in societal security efforts. This also applies to CBRNE emergency preparedness. It must therefore be ensured that civilian society has access to and routines for the Armed Forces' support in the form of expertise, equipment and advice. This is also one of the main measures in the national strategy for CBRNE emergency preparedness (2016–2020). Here it is determined that civil and military authorities will further develop the CBRNE cooperation. Cooperation will be based on the total defence concept with reciprocal support in peacetime, crisis, armed conflict and war. FFI will support this work.

If we are to achieve the objectives in the Long Term Plan and the CBRNE strategy, the strengthening of the CBRNE emergency preparedness must be based on knowledge and resources. At the same time, the defence sector is facing complex challenges that require a comprehensive approach. The strengthening of the Armed Forces' CBRNE emergency preparedness must therefore be viewed in the context of the Armed Forces' other duties, in order for the principles regarding capabilities and sustainability to be fulfilled across the entire spectrum of crises.

National and international cooperation

Through national and international cooperation, FFI will contribute towards increasing knowledge about future chemical and biological weapons and the consequences for the total defence. An important part of the efforts to strengthen the Armed Forces' defence against such weapons will be to strengthen the national CBRE emergency preparedness laboratory at FFI. FFI will also contribute with knowledge and expertise that is necessary in order to provide advice in connection with Norway's follow-up of the Chemical Weapons Convention, Biological Weapons Convention and the Australia Group.

International research cooperation

The technological challenges faced by the Armed Forces cannot be solved without international research cooperation. Research cooperation contributes towards the development of expertise that is significant for the Armed Forces' operational capabilities and that can also have positive spin-off effects for the Norwegian defence industry, economy and society. FFI is a key actor in Norwegian defence and security research and attends to several important national roles in relation to the international network. Based on the needs of the Armed Forces and in the sector, FFI both initiates and actively participates in cooperation to support knowledge development and innovation.

NATO and its close allies will continue to be the most important arena for international research cooperation. FFI will continue to prioritise activities under the NATO Science & Technology Organization and the EDA, in addition to the trilateral cooperation with the UK and the Netherlands, the SMART cooperation with the Netherlands, Nordic cooperation and bi- and trilateral cooperation with the USA, Germany, the UK and others.

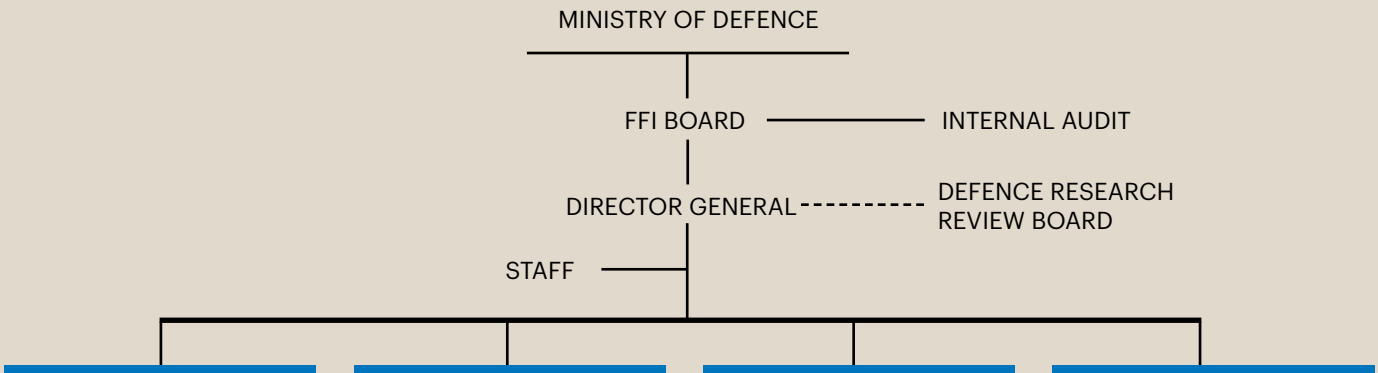
The EU is a key partner for Norway also in security and defence policy. The EU's work on a common security and defence policy is continuously developing. A close cooperation between NATO and the EU is essential for meeting the changes in the security policy, geopolitical and military situation. At the same time, there is broad political agreement in Europe that comprehensive supra-national changes must be made in order to reverse the negative developments in coordination and cooperation within military research, defence industry and military procurement that have been occurring for some time.

As a component in strengthening the European defence cooperation, the European Commission has proposed establishing a separate defence research project in connection with the EU's next Framework Programme for Research and Innovation (2021–2027). Norway is the only non-EU Member State that has been given the right to participate in the pilot project for defence research programme, "Preparatory Action on Defence Research". Together with the Norwegian defence industry, FFI will apply to participate in the in pilot project and in the upcoming defence research programme. This is a component of FFI's contribution to an effective and relevant Armed Forces and a competitive defence industry.

FFI will also utilise the opportunities for civil-military synergies and military utility values in EU civil research and innovation programmes. In 2021, Horizon Europe will replace the current framework programme, Horizon 2020. The European Commission has proposed a budget of EUR 97.6 billion for the next framework programme. This makes Horizon Europe the largest research programme in the world. FFI has had considerable success in Horizon 2020 and in previous framework programmes. In accordance with guidelines in the current Long Term Plan, FFI will continue the efforts towards EU projects in the fields of societal security, maritime, cyber and outer space.

Based on the needs of the Armed Forces and in the sector, FFI both initiates and actively participates in cooperation to support knowledge development and innovation.

ORGANISATION CHART



STRATEGIC ANALYSES AND JOINT SYSTEMS

- Cyber security and operations
- Electromagnetic operations
- Defence modelling
- Defence economy
- Operational ICT

DEFENCE SYSTEMS

- Autonomous systems
- Combat aircraft, missiles and ammunition
- Combat structures
- Ground forces combat systems
- Maritime combat systems
- Surveillance

COMPREHENSIVE DEFENCE

- Protection of society (BAS)
- CBRNE:
  - Chemical, biological, radiological and nuclear threats and defence
  - Improvised explosive devices
  - Dispersion modelling and nuclear threats
- Environment and health
- Fluid and materials
- Terrorism and asymmetric warfare (TERRA)

INNOVATION AND INDUSTRIAL DEVELOPMENT

- Asymmetric warfare
- Defence industry development
- Commercialisation and spin-off industry
- Center for innovation, concept development and experimentation (ICE worx)
- National and international research cooperation

EXECUTIVE GROUP

John-Mikal Størdal, *Director General* / Jan Erik Torp, *Chief of Staff*
Espen Skjelland, *Research Director of Strategic Analyses and Joint Systems Division*
Johnny Bardal, *Research Director of Defence Systems Division*
Janet Martha Blatney, *Research Director of Comprehensive Defence Division*
Hanne Marit Bjørk, *Research Director of Innovation and Industrial Development Division*

FFI turns knowledge and ideas into an effective defence

FFI KJELLER
PO Box 25
N-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

FFI HORTEN
PO Box 115
N-3191 Horten

Office address:
Karljohansvern
N-3190 Horten

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Military telephone: +47 505 70 00

E-mail: ffi@ffi.no

Text and design: FFI
Illustrations: FFI and Made by Cecilie
Print: 07 Gruppen
Circulation: 1500
P: ISBN 978-82-464-3132-1
E: ISBN 978-82-464-3133-8

www.ffi.no