FFI-RAPPORT

16/02449

Protecting Society in a New Era

–

Monica Endregard
Kjersti Brattekås
Kjell Olav Nystuen
Therese Sandrup
Wenche Gerhardsen

Protecting Society in a New Era

Monica Endregard
Kjersti Brattekås
Kjell Olav Nystuen
Therese Sandrup
Wenche Gerhardsen

Norwegian Defence Research Establishment (FFI) 23 March 2017

Keywords

Sikkerhet
Beskyttelse
Sivilt-militært samarbeid

FFI-rapport
FFI-RAPPORT 16/02449

Project number
1391

ISBN
P: 978-82-464-2906-9
E: 978-82-464-2907-6

Approved by
Kjersti Brattekås, *Research Manager* Janet M. Blatny, *Director*

Summary

Norwegian contingency planning and crisis management are based on a comprehensive national effort between a number of players spanning the entire spectrum of Norwegian society – civilian and military, public and private. Our society is constantly changing and developing, and with this, the social assets and technology in support of society changes as well. The threats to that society, the risks to it and its vulnerabilities are likewise constantly changing. Hence a vibrant and robust research community plays an important role in establishing a sound basis of knowledge and expertise upon which to develop Norwegian contingency planning and crisis management. This is accomplished through illuminating the dilemmas faced by policy makers and administrative agencies, proposing appropriate measures of action and responses, and contributions of knowledge and expertise to aid in policy making. Research provides up to date, realistic, critical and nuanced expertise on the functioning of Norwegian societal security and contingency planning.

In this issue we present some of the findings from FFI's research in the area of societal security and selected key research results from the 'BAS' project series on the protection of society.[1] FFI was a pioneer in carrying out research in civil preparedness, and with its BAS series of projects FFI broke new ground in what would later be referred to as research on societal security. Research in this field continues to develop at a number of Norwegian universities, colleges, and institutes and societal security has become established as a specific course of study at several institutions of higher learning. It remains a key area of research for FFI.

The long-term aim of the BAS projects is the realisation of a thoroughly developed concept to protect the population and society in general and to support the on-going prioritisation of protective measures. The thrust of today's BAS research examines major events and incidents that could impact Norway and which would require coordinated contingency planning and crisis management across differing sectors and levels. Certain types of crises would necessitate civilian-military and public-private cooperation, and as such, would require careful premeditation. We wish to contribute knowledge and expertise and convey as much as possible of our research findings to the public for the public good. However, precisely because this research does cast a critical view to the nation's crisis management and emergency preparedness and helps in pinpointing vulnerabilities, it is necessary to shield some of our findings.

The research group for the BAS project program is interdisciplinary in nature and consists of researchers from different fields and disciplines, including political science, social anthropology, chemistry, physics, information science, and engineering. The group cooperates with several other research groups at FFI, among them people working in the fields of long-term planning for the Armed Forces, terrorism research, cyber security, and protection from explosives, chemical, biological, radiological and nuclear threats.

[1] The project series is called Protection of Society, in Norwegian "Beskyttelse av samfunnet" - BAS

Sammendrag

Norsk beredskap og krisehåndtering er basert på en omfattende nasjonal dugnad mellom en rekke aktører — sivile og militære, offentlige og private. Samfunnet er i stadig endring og utvikling, og trusler, verdier og sårbarheter som til sammen kan si noe om hvilke risikoer samfunnet er utsatt for, endres også. Forskningsmiljøene har en viktig rolle i å etablere et godt kunnskapsgrunnlag for utvikling av norsk krisehåndtering og beredskap, for å belyse dilemmaer, foreslå tiltak og endringer og bidra til politikkutforming. Forskning bidrar med oppdatert, realistisk, kritisk og nyansert kunnskap om hvordan norsk samfunnssikkerhet og beredskap fungerer.

Formålet med denne rapporten er å presentere FFIs samfunnssikkerhetsforskning og utvalgte sentrale forskningsresultater fra prosjektserien Beskyttelse av samfunnet (BAS). FFIs forskning på sivil beredskap i starten av prosjektserien BAS brøt ny mark i det som senere kom til å omtales som forskning innen samfunnssikkerhet. Forskningen på dette feltet er i vekst ved en rekke universiteter, høyskoler og institutter i Norge i dag, og samfunnssikkerhet er etablert som en egen studieretning ved flere utdanningsinstitusjoner. Det er et viktig område for FFI å satse på.

Det langsiktige målet med BAS er å bidra til et gjennomarbeidet konsept for beskyttelse av befolkningen og samfunnet for øvrig samt å støtte opp under en løpende prioritering av beskyttelsestiltak. Kjernen av dagens BAS-forskning er å se på de store, alvorlige hendelsene som kan ramme Norge, og som krever beredskapsplanlegging og krisehåndtering på tvers av sektorer og nivåer, og der det er behov for sivilt-militært og offentlig-privat samarbeid. Vi ønsker å bidra med kunnskap på en god måte og sørge for å formidle mest mulig av våre resultater til offentligheten. Fordi forskningen bidrar til å belyse sårbarheter og har et kritisk blikk på vår krisehåndteringsevne, er det likevel nødvendig å skjerme deler av forskningsresultatene.

Forskningsgruppen for prosjektprogrammet BAS er tverrfaglig sammensatt av forskere fra statsvitenskap, sosialantropologi, kjemi, fysikk, informatikk og ingeniørfag. Gruppen samarbeider med en rekke andre forskningsgrupper ved FFI, blant annet innen langtidsplanlegging for Forsvaret, terrorismeforskning, cybersikkerhet og beskyttelse mot eksplosiver, kjemiske, biologiske, radiologiske og nukleære trusler.

Dagens BAS-forskning med tilhørende prosjekter og forskningsoppdrag finansieres av blant annet Forsvarsdepartementet, Justis- og beredskapsdepartementet, Nærings- og fiskeridepartementet, Direktoratet for samfunnssikkerhet og beredskap, Nasjonal sikkerhetsmyndighet, Norges forskningsråd, EUs 7. rammeprogram, Forsvarsbygg, Kystverket og Jernbaneverket.

Content

Preface

This report has been translated from the Norwegian “VITEN – Beskyttelse av samfunnet i en ny tid, FFI-rapport 15/02472”. We would like to thank Jennifer Høibråten who has translated this report into English.

VITEN is a new type of magazine from the Norwegian Defence Research Establishment (FFI). It is directed towards a broader audience and the material is presented in a straightforward magazine format. In the initial phase, VITEN is published four times a year and comprises part of FFI’s commitment to the dissemination of important research.

Through VITEN we hope to contribute to a more informed public debate through presentations of research-based expertise, thereby increasing public knowledge and fostering a deeper understanding of the issues. The topics for these reports come from the full breadth of FFI’s research – from military technical aspects to defence planning, security policy and societal security. We aim in particular to elucidate some of the challenges facing the armed forces and the Norwegian civil sector. It is our hope that VITEN will serve to generate interest in the many areas of research in which FFI is engaged, and demonstrate the ways in which FFI’s research contributes to a stronger defence and a more secure society.

An electronic version of VITEN is available on FFI’s website ffi.no. Other comprehensive reports and other material may also be found here.

Would you like to know more about VITEN? Contact us at VITEN@ffi.no

1 Civil Emergency Preparedness After the cold War

Since the close of the 1980s, understanding and cooperation between the military and civilian sectors of society on matters of societal security have been changing. Research in the field of civil safety has also been instrumental in powering this change. Through its project series *Protection of Society* (BAS), FFI has been an active participant in this field of research since its inception. The need for more research in the field began with the fall of the Berlin Wall and the drawing back of the Iron Curtain. These momentous events led to rapid changes in the way society perceives threats and responds to them.

With the end of the cold war, the fear of nuclear weapons and the possibility of a third world war gradually gave way to a more relaxed perception of what constituted a threat towards Norway. At the same time, the global internet and continual developments in information technology became a central factor in the flow of information in society. Developments in information technology and its application in society were extremely rapid, and in a very short time the internet provided unparalleled access to information. The relationship between the roles of the public sector and industry in society was also challenged in this period. Former heavy state enterprises such as telecommunications and power were de-nationalised and split up into new entities as a composite of state enterprise and private company. People no longer saw a need for doing things in the old way. Another consequence of this shift in thinking occurred in defence planning with the dismantling of the old Total Defence model, even though this concept was not based on any political or administrative decision. The origins and purpose of the Total Defence concept was an important backdrop for the BAS projects.

A contributing factor to FFI's decision in the mid-1990s to embark upon the BAS projects was the development in the civil sector. The formal background for the BAS project series is described in the Norwegian Parliament White Paper 24 (1992-93) and White Paper 48 (1993-94). These lay down the principle that civil emergency preparedness ought to be reorganised, both in light of an altered threat scenario and also to make better use of resources in peacetime. The need for a reassessment of civil preparedness was further underlined with the privatisation of certain companies in the public sector, such as parts of the Norwegian State Railway, Telenor and the power sector. New forms of ownership fostered new possibilities of cooperation between public, private and foreign participants, and this required new standards for contingency planning. Cooperation was initiated in 1994 between the former Directorate for Civil Preparedness (now the Norwegian Directorate for Civil Protection) and FFI to plan the reorganisation of civil preparedness in a more long-term perspective. The first BAS project was thus underway.

1.1 Foundations of a robust society

The first part of the project series, BAS 1, was completed in March 1997. BAS 1 established the importance of having contingency measures in place to cover needs during the initial weeks or months of crisis in the event of armed conflict. It became even more important to see the

connection between preparedness in peacetime and in times of armed conflict, and to protect individuals indirectly by protecting important societal functions. One tool for preparing society for possible adverse events is through the use of scenarios. Scenarios are descriptions of a conceived chain of events for the purposes of studying the consequences of different courses of action. Scenarios are an aid in identifying the holes and problem areas within the country's civil preparedness and they are useful in defining the goals of contingency planning. BAS 1 used both peace and wartime scenarios to demonstrate the kinds of situations that could arise and that an emergency preparedness system must be able to handle. Examples of war scenarios included the invasion of Finnmark and Northern Norway, along with raids and strategic assault on the country. Peacetime scenarios included natural disasters, traffic accidents, infrastructure fires, forest fires, oil spills, accidents while transporting hazardous materials, industrial accidents, supply crises, nuclear contamination, massive influx of refugees and acts of terrorism.

Picture 1.1 The Norwegian Armed Forces in Northern Norway (Photo: Forsvaret)

The most important societal functions to be maintained, both in armed conflict and in peacetime, were identified and defined in BAS 1. The project examined aspects of on-going developments in military technology and future warfare. The project also studied experiential data from the Gulf War of 1991 to see how the coalition forces attacked strategic targets and gauge the effect of these attacks. Furthermore, air warning systems and shelters were evaluated, and possible improvements to these protection systems were considered.

Concurrent with the BAS 1study were the topics “the vulnerable society” and “critical infrastructures” which were receiving increased attention at the international level. In the United States, the President’s Commission on Critical Infrastructure Protection released its report in 1997. This report emphasised the same points that the BAS project at FFI had posited. This helped to increase public awareness within Norway of the vulnerability of modern society. The American report pointed out key developments such as the rapid increase of complexity in society and the fact that the developments in themselves were so rapid that it was difficult to keep pace with them.

The analyses in BAS 1 established a basis of prioritisation for critical areas of infrastructure warranting closer investigation: telecommunications, the power supply, transportation, the oil and fuel supply, leadership and information. The first three areas on this list were followed up in ensuing BAS projects.

1.2 Telecommunications in peace and conflict

In the period between 1997 and 1999, the second in the series of BAS projects completed a thorough investigation of vulnerabilities in the public telecommunications system. The project concluded that problems in the telecommunications system would cause considerable friction in society, even if the problems only occurred in normal peacetime conditions. More specifically, without access to telecommunications, society as a whole and civil contingency planning would be unable to offer sufficient support to the Armed Forces.

BAS 2 identified specific areas of vulnerability in the public telecommunications network, and highlighted the consequences of a serious failure in this network. The project then proposed a set of strategies and remedial measures to protect the telecommunications network against different kinds of interruptions and challenges. For example, the closing report of the BAS 2 project suggested reversing the prevailing assumption that good safeguards against incidents in peacetime will also provide protection in times of conflict. The following guiding principle was suggested in its stead: “a telecommunications network that is well protected against manmade threats will also be well equipped to withstand normal events that occur in peacetime.”

Among the networks that came under scrutiny in the BAS 2 project were the public telecommunications network, the Armed Forces network, and the mobile communications network. The project concluded with the recommendation that Norway should pursue extensive safeguards for the public network rather than relying on services from the two alternative networks, *inter alia* by utilising the diversity between the various telecom operators to reduce vulnerability. The project also pointed out a new development towards the close of the last millennium: “In the future, we will see a convergence between landline services and mobile telecommunications services. It is therefore important that the mobile telecommunications network is also made robust.” Today this is a familiar topic.

Despite its modest size, the BAS 2 project received considerable attention. The Norwegian Ministry of Transport established a project entitled Telecommunications Preparedness in a Free

Competition Market (TIFKOM), a project intended to process the results from the BAS2 Project and ensure that the measures were actually implemented. White Paper 47 (2000-2001), which was issued some time later, became a cornerstone for the new regime of telecommunications and preparedness in Norway. Among the first measures to be implemented after the White Paper had been discussed in the Parliament was the establishment of an emergency preparedness and security function within what was then known as the Post and Telecommunications Authority. FFI was involved in all of these processes and received an immediate positive response to its research results. In spite of this encouraging start, the topic was only loosely followed up. A possible explanation for this may be because the Post and Telecommunications Authority moved to a new location, with an ensuing high turnover of expertise.

1.3 Our dependence on electricity

In the period 1999 to 2001, the BAS 3 project analysed the dependency of Norwegian society on electricity. The meaning of vulnerability in the telecommunications network and data security in general was clearly delineated in BAS 2.The BAS 3 project looked at measures that could be taken to reduce vulnerability in the power supply. The power supply system in Norway is vulnerable on a number of counts, both with respect to physical abuses and strains, and possible attacks on its information systems. The main thrust of the BAS 3 study was on examining events that arise in the grey zone between peacetime and a declared state of war between Norway and another state.

The BAS 3 project was finalised with the conclusion that in the future, the vulnerability of modern society would increase. In view of this and of a threat scenario that was more unpredictable, FFI recommended that information systems and telecommunications technology (ICT) be secured. Other key recommendations included investing in personnel and expertise, improving the possibilities for re-establishment and repair and the securing of critical functions in the national infrastructure. For the long-term FFI recommended instituting a high level of security for the power supply.

Virtually all electrical power production in Norway is in the form of hydro-electrical power which is transferred over cables, in the air, underwater and underground. Several power lines have been laid in the same trace line to preserve both the environment and resources. The disadvantage of this is increased vulnerability, in part because the infrastructure for the production and transport of power is difficult to monitor and protect. There was only limited interest to implement contingency measures among the actors in the power industry, and in view of this, FFI felt that there should be a sharp increase of public resources specifically earmarked for securing the national power supply. The national authorities carry a heavy responsibility, but the individual consumer of electricity can also do his or her part to reduce vulnerability by installing alternative systems for heating and emergency power.

The power sector still had a functional security and emergency preparedness regime at the beginning of the millennium, in contrast to the telecommunications sector where much of this

had eroded over time. Not long after BAS 3 presented its conclusions, the security and emergency preparedness regime in the power industry was strengthened even further.

1.4 Transportation in vulnerable times

The transport sector was the subject of the BAS 4 project that lasted from 2001 to 2003. BAS 4 was commissioned by the Directorate for Civil Protection (DSB), the Ministry of Justice and the Ministry of Transportation which were all seeking answers to the questions: how vulnerable is the transportation sector, and what can be done to make it more robust?

The assessments made in this project provided insight into systems in aviation, the railways, road-, and maritime transportation. The analyses showed that it would take a number of simultaneous terrorism events or acts of war to knock out the transportation capacity at a national or regional level. Nevertheless, BAS 4 found that some of the subsystems in the transport sector were more vulnerable than others, including the information and communications systems in logistics and traffic management, meeting points at terminals and the means of transport and transportation of hazardous materials. Another area of concern was the 'Transportberedskapsorganisasjon' [transport preparedness organisation] (TBO) which showed a serious lack of coordination in crisis situations. BAS 4 recommended that the Ministry of Transportation should take over this responsibility by establishing a forum for transport preparedness. TBO was closed down in 2005, and responsibility for coordinating contingency planning at the regional level was transferred to the county authorities.

Picture 1.2 *The Armed Forces and civil emergency preparedness agencies carry out an exercise together (Photo: Forsvaret)*

The BAS 4 project concluded that even though the Norwegian transport sector is reasonably robust, it is nevertheless critically dependent on other sectors such as telecommunications and fuel- and power supply. This applies in particular to the railway system. Besides, a move towards greater independence of ICT would alter the premises for contingency planning in the transport sector. The requirement of greater efficiency has the effect of increasing ICT use, both in mass transit and in the transport of cargo. This in turn increases vulnerability and results in fewer people who are capable of operating systems manually in the event of a crisis. Consequently, BAS 4 proposed introducing one of three security levels, depending on the security situation in Norway, with baseline security at the bottom (the cheapest alternative), followed by protection against terrorism (more expensive) and finally at the highest (and most expensive) level, protection against armed conflict.

BAS 4 accentuated how dependent we are on ICT services and the ICT infrastructure, and how vulnerable society is in view of this dependency. The project demonstrated the challenge in using good methods in sectorial risk analyses where ICT systems play a prominent role in overall vulnerability. As a result, the following BAS project researched methods of holistic analyses that included the vulnerability of integrated information systems.

1.5 Better methods reduce risk

The fifth BAS project was conducted in cooperation with different research institutions, academia, the authorities, and enterprises from both the public and the private sector. The earlier BAS projects laid down concrete proposals for cost effective measures that would reduce the vulnerability in the systems they studied. When BAS 5 started in the fall of 2004, it quickly became apparent that this time the actual methods behind the measures were the most relevant. The reason for this change was the rapid development in ICT as well as in technology and the market in general. As a result, concrete measures were often obsolete before they had even been implemented. Therefore BAS 5 endeavoured to find methods of assessing risk and vulnerability in all critical societal functions, not just in ICT alone.

A risk and vulnerability analysis is a tool for handling risk. Undesired events with serious consequences are identified and ranked according to the likelihood of occurrence. It is the first step on the road to reducing risk, in part because it ensures that the most important systems and most effective measures are prioritised in security work. The national strategy for information security from 2003 states that “all measures aimed at information security shall be based on analyses of risk and vulnerability.” BAS 5 carried out risk and vulnerability studies of existing ICT systems at a large hospital, a large financial concern, a major company in the power supply industry and a large concern in the petroleum industry to use as case studies. In these analyses, the project undertook a special study on the vulnerability of the internet. Other studies in the project looked at coming developments in nanotechnology, graph theory, and the role of the authorities in information security in terms of preventing and managing crises.

At the conclusion of the project in 2007, a methodology had been developed that could be used to identify and rank critical functions of society and ICT systems, carry out risk analyses of ICT

systems critical to society and assess the effectiveness of measures intended to reduce ICT vulnerability. These methods answered questions such as: what activities and ICT systems are most critical to society? How does one analyse risk and vulnerability in the critical ICT systems? How does one choose the best option for safeguarding vital ICT systems? Prioritisation is most meaningful for issues that are quite concretised. For example, this might be in answer to questions such as who should have priority access to communications services in a crisis, or where does it make sense to invest in crisis prevention?

There are many aspects in developing good risk analysis methods for ICT systems. That is why BAS 5 documented its experiences in an overall guideline when carrying out risk analysis of critical ICT systems. However, risk analysis is only one of several tools that are useful in augmenting ICT security. Making it a general requirement to carry out risk and vulnerability analyses as an element of bolstering national security makes little sense unless the agencies themselves understand why it should be done and how best to do it. The lessons from BAS 5 gave important insight into this. BAS 5 also recommended the establishment of a framework with a concrete ambition level for work with national information security, clarification of participant roles and tasks, and good methods at the base of everything.

In BAS 5 a number of professional topics were examined in the border area between ICT and risk analysis. This was ground breaking work, and it was natural to involve universities and colleges. The project provided greater insight into very complex conditions, while simultaneously demonstrating how a seemingly common topic of study can nevertheless manifest itself quite differently in different research environments.

2 The Total Defence Concept Today

The mutual dependency of the Armed Forces and civil society is on the increase. With this comes a need for cooperation in securing the safety of society in the total defence concept of today.

The idea of a total defence concept for Norway was developed by the government in exile in London during the Second World War. The idea was that the defence of Norway would be built on military defence and broad civil preparedness. This would safeguard Norway’s territory, independence, national interests and civilian population. In its original form, the total defence concept was tailored to meet an invasion, but it has been steadily revised and developed further to meet new challenges in the current threat scenario.

Picture 2.1 *Mass injury exercise in Narvik. The Armed Forces and civil emergency preparedness agencies carry out an exercise together. (Photo: Forsvaret)*

The modernised total defence concept is still based on the principle that Norwegian society ought to utilise its limited resources as effectively as possible in the event of a crisis. Mutual support and cooperation between the Armed Forces and the civilian society is a fundamental principle in safeguarding the security of society and the state, through the whole spectrum from peace to security crisis to armed conflict.

2.1 The need for mutual support

The Norwegian Parliament has made clear that all resources that are available in the event of armed conflict should also be available in the event of a crisis in peacetime. The Armed Forces will emphasise support to the civilian sector in peacetime crises to a much greater degree than before. It is one of the explicit tasks of the Armed Forces to participate in safeguarding society and other central societal roles.

The terror events of 22 July 2011 highlighted the need for military support to the civilian sector on very short notice. Upon request, the Armed Forces should be able to mobilise resources quickly and assist in case of accidents, natural disasters, events of serious crime and other peacetime crises, and to protect the country against serious impacts, including terrorist attacks. However, other forms of support should be considered as well, for example the societal need to maintain a robust civilian and military cyber domain.

Picture 2.1 *The government high-rise building in the government quadrangle was completely bombed out on 22 July, 2011. After the attacks flowers and candles were placed on the street. A soldier on guard duty in Oslo after the attacks of July 22, 2011 answers the questions of passers-by (Photo: Forsvaret)*

At the opposite end of the scale, civilian support to the Armed Forces should preferably be based on commercial arrangements and cooperation between civilian actors through contracts and agreements on supply and emergency preparedness. Here the Armed Forces have become more dependent on civilian vendors of infrastructure, goods, services, and technology. However, this kind of dependence could potentially impair the Armed Forces' efficiency in certain kinds of scenarios. With shorter warning times and longer lasting conflicts, this dependency becomes even more visible. Large scale obligatory support to the Armed Forces from the civil sector in situations of major crisis still requires the application of emergency legislation. This would no longer be necessary in a defence concept in which it is agreed that the Armed Forces shall also support the civilian society.

2.2 Complex new vulnerabilities

There have been widespread changes in the total defence concept over the last 20 years. This has come as a consequence of several factors: the new reality in international security in the aftermath of the Cold War, developments within the Armed Forces, new parameters within civil emergency preparedness and general developments within society itself. Concurrent with this is also the trend of increasing privatisation, globalisation and rapid development in technology –

not least within the field of information technology. For example, agreements have been made with private companies on the use of civilian fibre links in the ICT systems of the Armed Forces. This development, with more complex systems and terms of ownership, carry in themselves new forms of vulnerability. In peacetime as well as in times of crisis or armed conflict, foreign powers and other actors could direct strategic attacks against both the Armed Forces and society at large through advanced information operations, which could also be combined with other conventional means.

The development of the total defence concept is related to changes in security needs and our perception of the purpose of national contingency planning. The current emphasis is on the safety of society as well as the security of the state. The threat scenario has become more complex, all the more so because new perpetrators of terrorism are constantly emerging. The new threats are often more dynamic and lack limitations. These acts will often occur quickly and will consist of a combination of different means. It is more difficult than before to understand where the threats are coming from and what they concretely consist of. It is precisely in the face of this new threat scenario that cooperation between the Armed Forces and civilian society in the total defence concept becomes so important in the effort to protect society in the best possible manner.

3 What Do We Do If…?

From the start of the first BAS project in 1994 until the sixth project began in 2007, there have been enormous changes in the national effort to safeguard society. This is also the case for the nature of the challenges Norway and Norwegian interests face. Heading into the 1990s, the threat scenario was relatively straightforward, and a common scenario was a military attack against Norway carried out by the Soviet Union. A total defence concept was developed over time to respond to this threat. Today, however, the range of dangers and threats that Norway faces is much harder to grasp, and there are numerous events and incidents that could pose a threat against Norway and Norwegian interests. This makes the work to secure society complicated, for several reasons:

- There are no concrete challenges by which we can dimension and gauge our contingency planning and ability to respond to a crisis, especially at the national level. It is difficult to develop traceable work procedures that connect objectives and measures to a sufficient degree. How can we then determine what constitutes a sufficient level of preparedness in safeguarding society?

- There could be local interpretations of what constitutes the most important challenges, and problems in the coordination of contingency planning efforts between the various sectors and their various levels.

- The work could become reactive instead of preventive. Events that have already occurred receive great attention after the fact, while contingency planning for events that have not yet happened is not prioritised.

In common with the BAS 1 project, the BAS 6 project series developed and utilised scenarios to concretise the types of challenges Norway and Norwegian interests might face in the future. From this comes the possibility of determining the capacities necessary for handling the situation. One can then gauge the existing capabilities against the found needs and determine whether the current capabilities are satisfactory or not, pinpoint the capabilities that are lacking – and the possible consequences of this shortcoming.

Does today's work in security and emergency preparedness cover the whole spectrum of potential undesirable events? What types of events are not covered by existing contingency plans? Are we carrying out exercises focused on the right kinds of events? To be able to answer these questions, the BAS 6 project established a typology of all undesirable events that can threaten our security. Based on this typology FFI developed a set of scenarios for the work of safeguarding society.

3.1 Scenarios for safeguarding society

The project established a set of 20 scenarios describing complex courses of events that could have widespread consequences. The point of using scenarios is to gain input for discussion and to extend the mental map for the actors in the total defence concept. The scenarios give a starting point for discussion, table-top exercises, and emergency preparedness analyses among civilian and military actors. The scenarios cover such central aspects as crisis communication, civil military challenges, the international dimension and the role of industry through public-private cooperation.

FFI's scenarios were developed in parallel with DSB's national risk profile in 2011, and FFI and DSB had and continue to have a good dialogue in the work of developing scenarios. While DSB's scenarios are based on risk assessment with an emphasis on probability and consequence, FFI has strived to unfold the full spectrum of incidents which have serious consequences in order to cover scenarios that in the short term may seem improbable. The developed scenarios shall:

- be relevant for testing civil-military cooperation
- describe incidents which lead to major consequences
- describe incidents that could affect Norwegian interests, primarily in Norway
- be recognisable to both large and small municipalities so that both can relate to some of the issues faced

- include relevant scenarios for chemical incident preparedness as this topic has been selected as an area of study in national contingency planning

In the scenarios described, there are four phases in the course of events: build-up, acute stage, rescue stage, and normalisation. General questions have been developed for the scenarios to provide a basis for discussion and further analysis. There are also questions in every scenario for the purposes of jumpstarting discussions on emergency preparedness. The scenarios are also intended to serve as a tool to aid actors in the total defence model in organising table top exercises and group discussions on emergency preparedness and to foster greater understanding of their different roles. This is based on the assumption that the scenarios are used correctly. They must be developed further and be adapted to the specific purpose. A selection of scenarios in BAS 6 was used to analyse national preparedness and crisis management.

3.2 What happens in the event of an armed attack?

The scenario "armed attack" was used as the basis for an analysis of national crisis management and civil-military cooperation. The scenario describes a situation in which another state uses military force against Norway to assert its rights in the northern regions. The aim of the analysis was to study the degree to which the total defence concept was able to support the needs of both the Armed Forces and civilian society in such a situation.

The reorganisation of the Norwegian Armed Forces and civil emergency preparedness after the Cold War resulted in the civil sector concentrating on crises in peacetime, while the Armed Forces focused on operations abroad. Before and during BAS 6, the focus of attention was on the northern regions and the defence of Norwegian territory. It was therefore relevant to examine the consequences of these changes. Important questions were:

- Who has the overarching responsibility at the national level, and are the roles and areas of responsibility clear?

- Is there accordance between civil and military needs for resources (both personnel and materiel), and is there actual access to resources?

- Are the current national contingency plans up to date and have exercises been carried out in the relevant areas?

In an armed attack, the Armed Forces depend on support from the civilian society, inter alia for food supplies and fuel, heavy transport, for moving forces and maintenance capacity. The civilian society will feel the weight of increased demand and reduced manpower in this type of crisis collaboration with the Armed Forces. The public and private sectors will also have to cooperate much more than normal in order to transport injured people and repair destroyed infrastructure. The analysis showed that the necessary agreements were not in place for such collaboration. The authorities also lacked the proper planning to be able to receive NATO forces.

Picture 3.1 The Armed Forces (Photo: Forsvaret)

The analysis indicated that there were problems of cooperation between civil authorities and the Armed Forces both with respect to establishing and maintaining a common and updated overview of the situation, and in the question of responsibility for the safety of the civilian population. There were also considerable discrepancies between the civilian and military need for resources and availability in a crisis. Key findings included the following:

- The distribution of responsibility between different civilian actors remains unresolved.
- There is a discrepancy between the need for civil-military coordination and actual coordination.
- Even though current contingency plans exist, the departments themselves are not necessarily aware of this; they have also not carried out exercises.
- The civil authorities often lack access to classified network data. This complicates and delays the exchange of classified information.
- Civilian agreements and contingency plans to cover the needs of the Armed Forces for goods and services in an emergency have not been prioritised.

These challenges for the total defence concept were followed up in the BAS 7 project.

Picture 3.2 Civil – Military cooperation during an exercise (Photo: Forsvaret)

4 Understanding and Prevention of Radicalisation in Scandinavia

In the research project 'Searching the unknown: discourses and effects of preventing radicalisation in Scandinavia' (RADISKAN), researchers study the understanding and perceptions undergirding preventive work against radicalisation and violent extremism.

In Scandinavia today there is an on-going mobilisation and recruitment to different groups who resort to violence to attain political, ideological or religious goals. The Scandinavian countries have all developed their own plans of action against radicalisation and violent extremism. A common trait of the Scandinavian countries is the responsibility of civil society to identify groups that are susceptible to radicalisation and violent extremism. It is also considered the responsibility of local society and municipalities to implement preventive measures against radicalisation.

RADISKAN researchers are endeavouring to uncover what is happening at the grassroots level in view of the authorities having become more conscious of radicalisation. How does local society deal with the challenges of implementing preventive measures? RADISKAN also takes

a closer look at how potentially vulnerable individuals and groups are handled, and examines how definitions of radicalisation affect trust both between groups and inside groups.

4.1 No straightforward profile

The Norwegian government's plan of action against radicalisation and violent extremism from 2014 envisages a broad, preventive effort based on earlier experiences with general crime prevention work and work with right wing extremists. An underlying premise is a sort of marked trail from social exclusion – defined here as a lacking sense of belonging to Norwegian society – to radicalisation and further violent extremism and terrorism.

We lack knowledge about the causal relationship that the action plan cites, however. Studies of persons who have become radicalised and recruited into violent extremism suggest that there is no straightforward profile, and that preventing the processes of radicalisation will require different kinds of measures. There are calls for research that can shed light on the processes that lie at the heart of different kinds of radicalisation and extremism, both at the group and individual level. As of today, we simply do not have a good enough empirical foundation to develop targeted preventive measures.

4.2 Ethnographic fieldwork

The study has been financed primarily through the Research Council of Norway's Program for the Security of Society 2013-2018 (SAMRISK II). The project is led by FFI and is a collaborative effort that includes the University of Aarhus and FAFO, the Institute for Applied International Studies. The start date of the project was Autumn 2014 and it will run through to Autumn 2018. Through RADISKAN's various subprojects, ethnographic fieldwork will be carried out in Denmark, Sweden and Norway. A goal is to contribute to a greater knowledge of the challenges in preventing radicalisation processes.

Definitions in RADISKAN

RADICALISATION: A process whereby a person to an increasing degree accepts the use of violence to attain political, ideological or religious goals.

VIOLENT EXTREMISM: The activity of persons or groupings that are willing to resort to violence to attain their political, ideological or religious goals.

As may be seen in their threat assessments of the last few years, the Norwegian Police Security Service has become increasingly concerned about radicalised individuals and groups that are willing to resort to violence to attain their political goals. International conditions and conflicts outside of Norway have acquired great significance for the national threat situation, especially in terms of the so-called foreign fighters.

5 Comprehensive Security Without Myths

The analyses of national contingency planning that were carried out during the BAS 7 project were primarily focused on the upper part of the crisis spectrum. The analyses built further upon scenario work and studies that had been done in earlier BAS projects. In this project, research was carried out on the influences of technology on societal security, and some of the observations on this topic are included here.

Developments in technology can quite rapidly affect the vulnerability of modern society. This is often because we are becoming ever more dependent upon complex structures at the same time as we are less and less aware of the factual vulnerability of these systems. At the same time, we have new communications tools and decision support systems at our fingertips to facilitate effective crisis management. Faced with such velocity in technological development, we find ourselves feeling uncertain about how this affects our vulnerability and our ability to handle crises. A problem with this uncertainty is the multitude of myths that can arise. These myths can have a dramatic and potentially adverse effect on the overall security of society if they are not countered with sound knowledge. FFI is working hard to contribute to this more holistic understanding of security.

Picture 5.1 Civil-military cooperation (Photo: Forsvaret)

Electronic Communication (ECOM)

Developments in technology help boost the efficiency of society while simultaneously causing each of the critical societal functions to become more complex.

At the same time, we observe that ECOM is being used for more and more functions in society, and in several societal activities. The complexity and range of uses continue to grow.

This in turn leads to a situation where fewer and fewer people appreciate just how comprehensive and complex ECOM really is, and there is a lack of knowledge among the users of this advanced technology.

5.1 Crisis management in a digitalised society

In what way does technological development impact the vulnerability of a society? FFI has studied and analysed the connection between increased dependence on electronic communication (ECOM) and our leadership and crisis management in serious crisis situations.

Modern society has become completely dependent upon ECOM for day-to-day operations. To an ever-increasing degree, we have taken into use and become dependent upon new ways of communicating, both in the workplace and in the private sphere. Everyone has a mobile telephone, more and more people are using quite advanced applications, and we collect and share information using internet-based services. Interruptions to the mobile telephone service and the internet are quite common, leading to inconvenience and difficulties for us, both as individuals and enterprises; however, for the most part we have been able to handle these occasional lapses without their having any serious or lasting consequences. In normal situations, as long as no other serious events occur at the same time, society can manage to cope with these occasional glitches.

Norway's total defence concept, its national crisis management and civil preparedness have become quite dependent upon ECOM services to respond to national and international crises. At the same time, we know that ECOM services themselves are completely dependent upon a functional supply of power in order to work. Society's dependency upon extremely complex services such as ECOM and the supply of power has been permitted to grow unchecked with no thought given to the concomitant problem of even greater vulnerability. This vulnerability has now become visible through incidents such as the Lærdal fire and the storm Dagmar.

We have utilised a scenario-based analysis to gain insight into this state of affairs. The analysis identifies those ECOM services we would depend upon in a concrete, grave challenge for the country, for example during the crisis period in the aftermath of an external threat. The underlying theme has been protection of the civilian population and identifying the

vulnerabilities that ECOM services may inflict on our ability to manage the crisis. The scenario we have used as a starting point for data collection is a plausible national security crisis in which there is an imminent risk of armed attack in the northernmost region of the country.

Based on this scenario and employing a five-step approach, we identified the relevant crisis management actors at the local, regional and national level, and examined the way in which they are organised. We gauged the degree of interrelation between them and assessed the need for and role of communications in solving important tasks. This included looking at the means of communication available and utilised by these actors. We accomplished this by playing out the different phases of the scenario for pertinent actors in two municipalities and at the county level. Furthermore, we interviewed actors at the strategic level. We systematised the information in complex charts of communication between the actors at the local, regional and strategic level. The charts showed what methods of communication the actors used in the different phases as the situation developed.

The available service platforms are the telephone (both mobile and landline), internet, military ECOM and other cellular networks. The survey revealed where there was a need for ECOM and where the burden on ECOM was greatest at different times throughout the crisis. The geographical distance between actors who must interact almost continually throughout the crisis is so great that ECOM is the only means of communicating – thereby making ECOM an essential tool and vital to management of the crisis. The study showed beyond all dispute that the mobile telephone would be the most important communications service, and this would be true even in the most serious crises Norway could face. Alternative services such as the newly implemented emergency network (Nødnett) and military communications services would have limited usefulness in such a setting, in part because the user group is too narrow.

Central actors in this and other major crises include the chief of police, the county governor and other leadership figures in the county emergency council. To attain effective coordination and strengthen crisis management, the actors must have access to communications services that are both secure and robust. In a time when various forms of cellular technology and the social media are becoming an important supplement to traditional broadcasting services, it also becomes increasingly important to develop secure and robust information channels that are capable of reaching the various segments of the population. The most important conclusion of the survey is that mobile telephones are the only common means of communication that exist between the total defence actors in the national crisis management, the county governor, crisis management at the municipal level, the emergency response agencies, the healthcare system and the Armed Forces.

The use of such a basic approach revealed that backup systems such as satellite telephones and other forms of dedicated radio networks often lead to complacency and create the illusion of redundancy. In practice, it would be difficult to utilise these kinds of backup systems in a concrete situation of crisis because they are seldom used in exercises, because of the difficulty in quickly obtaining the contact information of the other actors, and because many of the other actors in the crisis management lack corresponding capabilities. This is an example of an area in which myths can arise, and which in extreme consequence, could have very serious implications

for the safety of society. This is a development that will become more reinforced over time if we are not alert and able to acquire the appropriate knowledge.

FFI's study shows how the development of technology and new ways of utilising that technology also carry new areas of vulnerability. The widening gap between users and their comprehension of the technology, upon which they are becomingly increasingly dependent, is a major component of the challenge. Because technological services have become so complex at the same time as the user interface is so well developed, the average user has little understanding of the underlying infrastructure or technology behind the services. This lack of technological knowledge translates to a lack of insight and comprehension of the vulnerability and relationship between services.

5.2 The need to see systems in correlation to each other

How does one measure a society's ability to handle a crisis? This could be quite a challenge seen in light of the Norwegian sectorial responsibility, that is to say, the differing realms of responsibility under the auspices of the respective ministries. How can we then ensure a holistic approach to contingency planning and the security of society?

ICT is an integral part of the vital services in all kinds of decision support processes within the realm of contingency planning and crisis management. It is also an integral part of such vital infrastructure such as the water and electricity supply and transport services. Systems of preparedness and infrastructure can both be hit more effectively through attacks against their data and communications systems. What then are the possibilities of these systems being affected, and how serious would the consequences of this be for the delivery of water, electricity, transport services and other vital services to society?

In order to fully comprehend the vulnerability and real risk that such a threat poses to society, it is vital to appreciate the increasing complexity with which today's physical systems and ICT systems are constructed. A concrete example illustrates possible challenges connected with a holistic approach to security, and the difficulties that can arise if a limited revision is used as a template for security. This example is from the infrastructure in the water and wastewater services in a large Norwegian city. The infrastructure for the water supply consists of physical infrastructure, that is to say, a water reservoir, treatment plant, elevated water storage tanks, piping system, pumps and more. This physical infrastructure is for the most part controlled by ICT systems, although not entirely. The water pressure in the pertinent system is attained through elevation changes and gravity, and not through ICT-controlled pumps.

A review of the system's ICT security revealed that a number of these systems have some serious deficiencies, and they are not protected well enough from intruders. This means that intruders could break in to the ICT system, an event that could have potentially serious consequences. The ICT review drew the conclusion that this was a method attackers could use to disrupt the delivery of water to the population, without having to go further into the system as a whole.

Despite the conclusions of the review, we found that barring short intervals, it was unlikely that an attacker would be able to impair the water plant's ability to deliver a safe water supply and ensure safe waste water treatment by means of an attack on a plant's ICT systems. The condition of the ICT is obviously unsatisfactory, but the system as a whole nevertheless has a sufficient number of 'mechanisms' in place to prevent serious consequences to the physical infrastructure. Weak ICT security could still be a problem for so essential a service as the water supply. The drinking water supply is a service in which society rests enormous confidence, and fear over the safety of the water supply could be a greater challenge with which to contend than a technical breach in the delivery system.

FFI's work showed that physical protection of society's systems of infrastructure is extremely important, both with respect to attacks on the ICT system and attempts to poison the water supply. A one-sided focus on rectifying system engineering deficiencies in ICT security while failing to view the security of the infrastructure as a whole could have an unfortunate outcome for users of the water and waste treatment system. Also in this case we can see that misconceptions about vulnerability and security can affect security work. ICT-based infrastructure is a highly complex area that is inaccessible to many; hence, the breeding ground for misconceptions is great.

An important conclusion is that it is vital to comprehend the interaction between advanced physical infrastructure and ICT infrastructure in order to evaluate overall security. Those who assess the security and vulnerability of systems must be able to acquire sufficient depth and breadth knowledge about the enterprise or system of infrastructure. The most important assets in the system as a whole must be identified. Otherwise, we risk misinterpreting our own risks and prioritising resources incorrectly. This example from the water sector shows what the lack of a holistic view can lead to when it comes to assessing security and crisis management.

5.3 It was easier in the old days

What then are the most important assets in our society today? One factor that has made it even harder to assess overall security is that the assets of society are now spread out more widely than before. Some of society's assets lie in the hands of public civil authorities and military authorities, but it is not only limited to them. To a large degree, the assets of society lay in the hands of private industry, under Norwegian and, to an increasing degree, foreign ownership. In the old days, it was simpler; the largest and most important assets were our defence secrets and the threat situation was stable. In step with the development of society, our assets continue to grow and become more intertwined. Developments in global society have led to a less transparent and less predictable threat scenario. More assets and the unpredictable threat scenario make us vulnerable.

BAS 7 concluded that the increased technological dependency on electronic communication results in a greater degree of vulnerability in national crisis management. BAS 7 also carried out other studies. The contingency planning of the Armed Forces was thoroughly examined, and studies were carried out on the cooperation between the police and the Armed Forces. National preparedness for chemical, biological, radiological and nuclear (CBRN) threats was assessed, and also measured up against the European society and public communication in crises such as these. Protection against high energy microwaves was also a part of BAS 7. In addition, exercises and evaluations of exercises were also project topics, and this work is being further expanded upon in the on-going BAS 8 project. An example of a concrete crisis management study carried out during BAS 7 was the study on the ash cloud crisis in 2010.

Picture 5.2 *From June 7-11, 2015, civilian and military partners collaborated in the exercise Oslo fjord. The aim of the exercise was to augment societal security. The task force Polar Bear VI and the police worked together to secure the police headquarters in Østfold county. (Photo: Forsvaret)*

6 Handling the Ash Cloud Crisis

Picture 6.1 *Av Boaworm - Eget verk, CC BY 3.0, (Photo: https://commons.wikimedia.org/w/index.php?curid=10026499 (Wikimedia))*

In April 2010, European aviation was impacted by the eruption of the Icelandic volcano Eyjafjallajökull. The situation required crisis management and cooperation between civil and military agencies, and became a situation that we can learn from.

The lack of an empirical basis from real life incidents for relevant crises in the upper scale of the crisis spectrum is a challenge. The alignment of national, regional and local crisis management should be as equal as possible in peacetime, crisis and times of armed conflict cf. the principle of equality. To the degree that there are experiences from real life events that we can draw upon, we should of course do so.

The spreading of the ash cloud led to the entire airspace over Norway being closed on Thursday, April 10, 2010. The restrictions on aviation and flying activities created challenges for the Norwegian healthcare system, especially in Northern Norway which depends heavily on air ambulances. The ash cloud crisis triggered the release of military support to health sector preparedness in Northern Norway. Furthermore, there were useful lessons to be learned from the handling of this crisis because it necessitated cooperation and coordination between a number of authorities and other agencies, both nationally and internationally.

SUCCESS CRITERIA FOR GOOD CRISIS MANAGEMENT

Recognise the crisis

Establish crisis management

Clarify roles and responsibility

Involve all concerned parties (public/private, civilian/military)

Involve professional communities

Continual updating of the situation overview

Establish cooperation forums (at local, regional, national, and international level)

Establish a coordinated communications strategy

Prepare and implement actions, including assistance programs

6.1 Authorities on the scene at an early stage

Generally speaking, the Norwegian authorities and the affected actors handled the ash cloud crisis in a good way. The authorities were quick to establish a central crisis management team and to establish coordination at a central and national level in the Crisis Council. The Ministry of Transport was appointed to lead the work. Eight ministries, the Office of the Prime Minister and six other public agencies participated in the Crisis Council. The net result of this was that the crisis management of the central authorities emerged as unified, well founded, and the information disseminated from the ministries was well coordinated.

The aviation industry emerged from the crisis in good shape for the most part. The industry was successful in communicating with other authorities and keeping them informed, and this also extended to private actors, the media and the general public. The principal elements of uncertainty were concerned with measurements and the prognoses for ash spreading in the air and the potential consequences of this for aircraft. The authorities adopted a cautious, restrictive approach, an attitude of “better safe than sorry” and closed the airspace. This decision was later reversed and the airspace was transformed into a three-zone regimen. Health preparedness in Northern Norway was strengthened both by reinforcements from the regional health authorities in Southern Norway and the use of military resources. Civil-military cooperation was strengthened and improved during the ash cloud crisis.

6.2 New initiatives after the crisis

In the aftermath of the ash cloud crisis, the different kinds of lessons learned have led to new initiatives. Examples include the establishment of a separate agency for volcanic ash, alternative emergency routing for buses in Northern Norway, research on and development of ash sensors on aircraft, and unmanned drones that can measure the level of ash in the sky. Furthermore, a video-based emergency medical conference was developed in the health sector and there are now numerous international initiatives to improve knowledge about volcanic ash and its effect on aircraft engines. Social media became an important information channel for the airline companies. Numerous actors such as the office of the County Governor of Finnmark, for example, recognised the usefulness of social media in communicating with the public and employed this communications channel in the fall of 2012.

What were the success criteria for good crisis management as exemplified by the authorities' handling of the ash cloud crisis? The authorities recognised the crisis in the early stages and established crisis management in which the affected parties, both public and private, civilian and military were involved. Roles and areas of responsibility were agreed upon and the Ministry of Transport was established as the ministry in charge of managing the crisis. The authorities were continually updated about the situation. Professional environments were consulted and remained involved throughout the crisis. The authorities established the necessary coordinating fora locally, regionally, nationally and internationally. Communication with the media and the public was unified and well-coordinated. This points to a clear and well planned communications strategy. Initiatives and assistance measures were implemented to handle the flight ban. This was particularly important in our northernmost counties where the dependency on aviation is great.

7 That Which Has Not Yet Happened

The technological development of the previous few decades has led to drastic changes in society and this affects threats and vulnerabilities. Consequently, we cannot assume that our understanding of societal security based on earlier events and incidents will be a good enough foundation upon which to meet the challenges we may face in the future. To handle something that has never happened before, we must know how systems work and what is potentially vulnerable. We must be able to identify and understand areas that are developing rapidly and could lead to sudden or unexpected challenges. With a greater comprehension of risk, vulnerability and threats in a modern, developing society, we are better equipped to meet future challenges to societal safety.

Because the developments we face are becoming increasingly more complex, cooperation between different actors across different sectors has become necessary in order to find solutions.

The on-going BAS 8 project focuses on the needs and systems of cooperation between the civil and military sector, and participates in cross-sectoral exercises. There is much work to be done in these areas before we have good systems in place for a holistic societal security tailored to the needs of a modern society.

BAS 8 is studying civil-military crisis management and contingency planning, and the research is based on the need to further investigate the issues that were brought up in BAS 7 as well as a number of new areas. The work with and FFI's contribution to the Chief of Defence's professional military council (FMR 2015) has also been instrumental in the design of BAS 8.

7.1 Societal needs are changing

A more dynamic threat picture requires innovative thinking on questions of societal security. Threats against society are in constant development, and the threats today can have different impacts than previously. An ever-increasing dependency on technology makes society vulnerable to cyber threats. The activities of the Armed Forces are also vulnerable to cyber threats. Cyber threats can be aimed at a number of different systems and services that are important to everyone, from the single individual to businesses, industrial activities and the Armed Forces. It is an interesting development that military and civil infrastructures for the dissemination of information are in the process of merging at the same time as these infrastructures have become global.

Things are happening much faster, and this in turn requires a much more rapid response. It is a development that confronts Norway with new challenges. The new threats the country could face will be dynamic and multifarious, to a much greater degree than before. In many instances, it will be possible to set them off with very short warning times, and they could consist of complex combinations of very different means. The threats will also develop more rapidly, and it will be much harder than before to understand the origin and content of the threats beforehand. It is no longer a given that a state actor with hostile intentions will declare war and use conventional methods against an opponent in uniform. The actors could be anything from individuals to groups and state actors. Their intentions, means and goals may vary. Threats in the cyber sphere will be particularly difficult to trace. It is thus extremely important that the public administration is able to meet whatever comes in an effective manner, and that it is able to do so rapidly. This is largely a matter of an increasing need for a stronger intelligence-based, analytical approach with a corresponding organisation and expertise. Effective coordination across the current levels of administration and authority areas will be very important.

The BAS research will contribute to an increased understanding of changing parameters and conditions for societal security and for thinking ahead in cooperation with the actors. The eighth project in the BAS series examines the overarching issues from the earlier BAS projects, both in light of social developments and new research developments. By carrying out research in four main areas, the project will be able to suggest ways in which society – both the civil sector and the defence sector – can cooperate on societal security. In the aftermath of July 22, 2011, a new principle of crisis management was introduced: cooperation. Cooperation and coordination are

necessary to meet complex challenges requiring the intervention of several departments, underlying agencies and actors simultaneously. There are many challenges with cross-sectoral cooperation and support between actors that require better understanding and planning if cooperation is to work in practice. The research that BAS is carrying out will elaborate further upon these challenges.

Picture 7.1 Civil-military emergency response exercise (Photo: Forsvaret)

The four main areas of research in BAS 8 are support to the Armed Forces from the civil sector, critical infrastructure and critical societal assets, crisis management exercises and civil protection measures. Effective and holistic contingency planning and crisis management entail mutual support and cooperation between the Armed Forces and civilian society in the whole crisis spectrum. This requires a clear allocation of responsibilities, cooperation, and communication in the management of crises and in the utilisation of collected societal resources. In BAS 7 we identified several areas within the realm of logistics and supply-preparedness which should be improved, and this is further addressed in BAS 8.

There have been major changes in the framework assumptions of the total defence concept since the end of the Cold War. BAS 8 will work towards providing a better knowledge base about mutual civil-military cooperation within the total defence structure, with an emphasis on support and logistics from civilian society to the Armed Forces in crises of national security and armed conflict. Furthermore, BAS 8 will examine critical infrastructure and critical societal resources to gain a holistic national understanding of critical societal resources that are worthy of protection in view of their importance to national security. Complex infrastructures such as the

electricity supply, telecommunications networks, transportation networks and information/leadership are the principal topics of this research. The approach and methodology of the research are important tools in assessing vulnerability, risk and contingency planning for complex infrastructures of society. We will develop this methodology further. A main question is the extent to which a comprehensive presentation of national risk, threats and vulnerability is attainable, and this is something we will endeavour to attain. A better knowledge base can result in better risk management, design and prioritisation of holistic and balanced measures of protection.

By commission from the civil protection division of the Directorate for Civil Preparedness, BAS 8 also addresses a concrete study of society's need for civil protection measures. In this study, we will make use *inter alia* of relevant information bases from earlier BAS projects, and the findings will be evaluated and updated. The main question is: what civil protection measures does modern society require in view of the current threat and risk situation? In the study, we will also examine shelters and the existing population warning regime. In BAS 1, a study was made of shelters and air warning, and the findings from this study are now, after almost 20 years, ready for review. We are now bringing up many of the same problems, but with a broader perspective that covers the whole crisis spectrum and takes into account societal changes since the 1990s.

7.2 Exercises of cooperation and coordination between the different sectors of society is necessary

Exercises and practice are the keys to successful cooperation between the different sectors. An important foundation for effective preparedness in a society is cross-sectorial crisis management exercises where the actors practice coordination within certain scenarios. The project will research exercises and the effect of exercises in addition to methods of planning, carrying out, evaluating and drawing lessons from trans-sectorial exercises. One of the flaws that became apparent in several of the exercises performed earlier was the lack of follow-up and experiential learning. Why is it that the identified lessons from completed exercises are not being followed up? Why do they not result in the desired learning? What is necessary in order to design effective exercises for coordinated training between the Armed Forces and emergency preparedness actors in the civil sector? What will give a feeling of mastery and imbue in the actors a culture of coordination?

Many participants from different sectors are involved in cross-sectorial exercises, such as the emergency services, the Civil Defence and the Armed Forces, as well as various directorates, agencies and ministries. In this research, we will consult organisers and exercise participants on the goals of the exercise, the methods by which it is carried out, and the results and lessons learned. We will use both national and international exercises as a basis for the study. The study will place particular emphasis on how lessons learned from exercises can best be applied in the form of improvements in organisations and planning. The project will then provide advice and recommendations to the Armed Forces and civil authorities.

FFI will further develop a good knowledge base through the BAS 8 project in order to strengthen civil-military cooperation within the total defence structure in times of crisis. This particularly applies to civil support to the Armed Forces. We will also discover better methods of understanding risk and vulnerability, especially concerning mutual dependencies in critical infrastructures and critical societal resources.

BAS 8 also aims to help make better use of cross-sectorial exercises. Our research could help the civil authorities and the Armed Forces to learn from experience and improve their practices following exercises. The research activities in BAS will contribute to strengthening the security of society in Norway.

References

Birkemo, G. A., Grunnan, T. & Nystuen, K. O. (2015). Kommunikasjon mellom totalforsvarsaktører i en kompleks sikkerhetspolitisk krise. FFI-rapport 2015/00372 (Begrenset), Kjeller, Forsvarets forskningsinstitutt.

Forsvarets forskningsinstitutt (2014). FFI-FAKTA: Krisehåndtering i et sårbart cybersamfunn. Kjeller, Forsvarets forskningsinstitutt.

Forsvarssjefens fagmilitære råd (2015). Et forsvar i endring. Oslo, Forsvaret.

Fridheim, H. & Hagen, J. M. (2007). Beskyttelse av samfunnet 5 (BAS5): Sårbarhet i kritiske IKT-systemer — Sluttrapport, FFI-rapport 2007/00874. Kjeller, Forsvarets forskningsinstitutt.

Fridheim, H., Hagen, J. M. & Henriksen, S. (2001). En sårbar kraftforsyning. FFI-rapport 2001/02381. Kjeller, Forsvarets forskningsinstitutt.

Hagen, J. M. & Nystuen, K. O. (1999). Beskyttelse av samfunnet med vekt på offentlig telekommunikasjon. FFI-rapport 99/00240. Kjeller, Forsvarets forskningsinstitutt.

Hagen, J. M., Fridheim, H. & Grunnan, T. (2010). Sikkerheitspolitisk krise, nasjonal kriseleiing og sivilmilitært samarbeid. FFI-rapport 2010/01009 (Begrenset). Kjeller, Forsvarets forskningsinstitutt.

Hagen, J. M., Knutsen, B. O., Bjørnenak, M. & Sandrup, T. (2011). Scenarioer for samfunnssikkerhet og nasjonal beredskap, FFI-rapport 2011/00648 (Begrenset). Kjeller, Forsvarets forskningsinstitutt.

Hagen, J. M., Rodal, G. H., Hoff, E., Lia, B., Torp, J. E. & Gulichsen, S. (2003). Beskyttelse av samfunnet med fokus på transportsektoren. FFI-rapport 2003/00929. Kjeller, Forsvarets forskningsinstitutt.

Hæsken, O. M., Olsen, T. G. & Fridheim, H. (1997). Beskyttelse av samfunnet (BAS): sluttrapport. FFI-rapport 97/01459. Kjeller, Forsvarets forskningsinstitutt.

Innstilling til Stortinget 234 (2003-2004) til Stortingsproposisjon 42 (2003-2004). Oslo, Forsvarskomiteen.

Innstilling til Stortinget 49 (2004-2005) til Stortingsmelding 39 (2003-2004). Oslo, Forsvarskomiteen.

Justis- og beredskapsdepartementet & Forsvarsdepartementet (2015). Støtte og samarbeid. En beskrivelse av totalforsvaret i dag. Oslo.

Løkken, K. H., Grunnan, T. & Birkemo, G. A. (2015). Muligheter og begrensninger ved kommunikasjonssystemer for bruk i krisehåndtering. FFI-rapport 2015/01453. Kjeller, Forsvarets forskningsinstitutt.

Maal, M., Endregard, M. & Birkemo, G. A., (2012). Askeskyen fra vulkanutbruddet på Island i 2010 — norsk krisehåndtering og noen erfaringer. FFI-rapport 2012/01319. Kjeller, Forsvarets forskningsinstitutt.

Meyer, S. (2009). Typologi over uønskede hendelser. FFI-rapport 2009/00447. Kjeller, Forsvarets forskningsinstitutt.

NOU (2000:24). Et sårbart samfunn. Utfordringer for sikkerhets og beredskapsarbeidet i samfunnet. Oslo, Justis- og politidepartementet.

NOU (2006:6). Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske informasjonssystemer.

Oslo, Justis- og politidepartementet. Stortingsmelding 24 (1992-93). Det fremtidige sivile beredskap. Oslo, Justis- og politidepartementet.

Stortingsmelding 29 (2011-2012). Samfunnssikkerhet. Oslo, Justis- og beredskapsdepartementet.

Stortingsmelding 37 (2004-2005). Flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering, Justis- og politidepartementet. Oslo, Justis- og beredskapsdepartementet.

Stortingsmelding 47 (2000-2001). Telesikkerhet og – beredskap i et telemarked med fri konkurranse. Oslo, Samferdselsdepartementet.

Stortingsmelding 48 (1993-94). Langtidsplan for det sivile beredskap 1995-98. Oslo, Justis- og politidepartementet.

Stortingsproposisjon 48 (2007-2008). Et forsvar til vern om Norges sikkerhet, interesser og verdier. Oslo, Forsvarsdepartementet.

The President's Commission on Critical Infrastructure Protection (1997). Critical Foundations: Protecting America's Infrastructures. Washington DC.

Read more at www.ffi.no/BAS

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

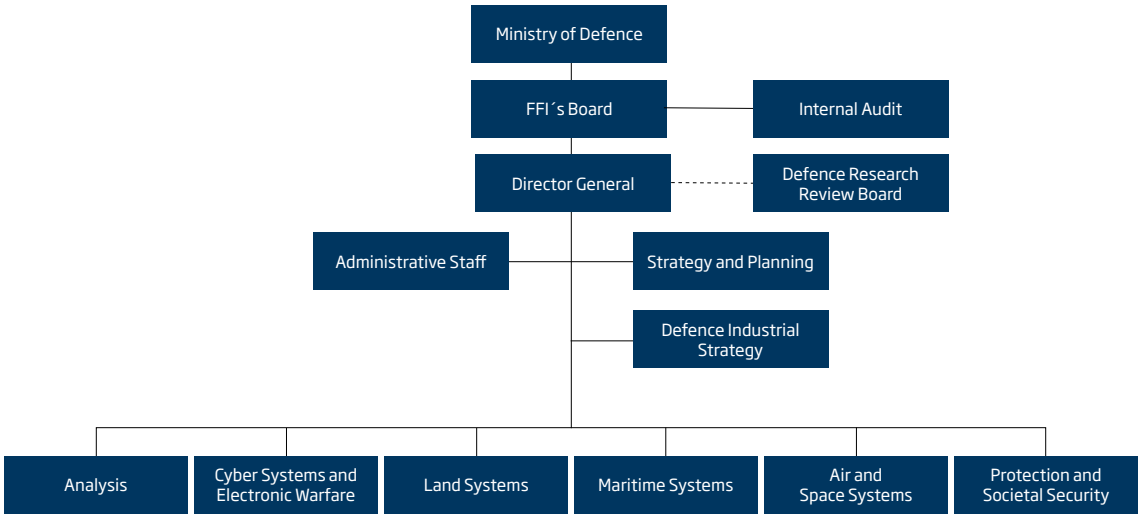
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no

FFI Forsvarets forskningsinstitutt
Norwegian Defence Research Establishment