Strategic outlook 8

Sweden's total defence – challenges and opportunities

Niklas H. Rossbach, Josefin Öhrn-Lundin, Daniel K. Jonsson, Anna Sundberg, Sofia Olsson, Jakob Gustafsson and Camilla Trané (eds.)

FOI-R--4802--SE

September 2019

FOI

FOI

Strategic outlook 8

Sweden's total defence – challenges and opportunities

Niklas H. Rossbach, Josefin Öhrn-Lundin
Daniel K. Jonsson, Anna Sundberg,
Sofia Olsson, Jakob Gustafsson
and Camilla Trané (eds.)

September 2019

FOI-R--4802--SE

ISSN 1560-1942
Printed in Stockholm 2019 by the Swedish Defence Research Agency, FOI
Cover: Trons / TT
FOI-R--4802--SE
Approved by Lars Höstbeck

Contents

Sweden's total defence – challenges and opportunities

Preface

This year's Strategic Outlook marks a decade of the Swedish Defence Research Agency (FOI) publishing this particular kind of report, which is intended for decision makers, those involved in defence, as well as the general public. It is also the first of its kind where the total defence is in focus. The concept of total defence includes both the civil defence and the Swedish Armed Forces. Nevertheless, in this report the focus is mainly on the non-military aspects of the total defence. The following chapters give a flavour of the agency's wide array of research areas.

The development of Sweden's restarted total defence is a central task for society. A new total defence is necessary to prepare Sweden for various types of disruptions, conflicts, and the worst-case scenario, war. The reason for reintroducing the total defence is, of course, the deteriorating international security situation.

The tasks of the civil defence include the protection of the civilian population, maintaining the continuation of the most important societal functions, and support for the Swedish Armed Forces. Unlike the Swedish Armed Forces, civil defence does not have one single central authority. Instead, it consists of the diverse activities that make our society function on a daily basis, such as food and energy supply, banking and payment systems, healthcare systems, as well as municipal activities, including the emergency services. The civil defence will be based on peacetime emergency preparedness, but in case of the highest state of alert being activated, the total defence will primarily consist of the societal activities that are needed at that time.

This year's Strategic Outlook also points to the need for civil defence to handle various forms of non-military aggression. One example is influence operations, which do not need to be part of open armed conflict. In other words, such attacks can take place in the so-called grey zone, between war and peace.

In order to create an effective total defence, in-depth knowledge of several different areas is needed, such as defence and security policy, crisis management, military technology, critical infrastructure, information security, and protection against dangerous substances. FOI's assignment is to provide such knowledge.

Over many years of research and development work, FOI has established a body of knowledge that is a resource for all parts of society. This edition of Strategic Outlook reflects FOI's research, as well as its knowledge of total defence issues. I hope that the report will be thought-provoking.

The authors discuss various aspects of the total defence. Chapters 1 to 3 form a background for the other sections, showing how global trends have led to the need for a total defence adapted to our time, and the importance of utilising experiences from the 1990s, as well as the importance of planning ahead when establishing a new total defence.

Chapters 4 to 6 are concerned with what is needed to allow total defence efforts to work in a satisfactory way in the coming years. Amongst other things, this is about motivating citizens to contribute to total defence, what is usually referred to as the will to defend. There is also a need for authorities to work together effectively; if cooperation is prepared in peacetime, it usually works better in a crisis.

Chapters 7 and 8 deal with various economic aspects of total defence. They show how Sweden is wrestling with investing the defence budget in the right capabilities, i.e. those needed for the future. These chapters also deal with the role of the business sector, and how cooperation between authorities and private companies can solve some of the challenges that arise when total defence capabilities are expanding.

Chapter 9 is the first of the chapters that focuses on technology and deals with how synthetic biology can strengthen the defence of Sweden, but also how, if in the wrong hands, it can give rise to new threats. Perhaps in a few years' time this area will be as talked about as cyber is today.

Chapters 10 to 14 deal with different perspectives of what, in the public debate, is associated with the internet, and increasingly with digitalisation or cyber. These chapters cover the importance of exercising cyber defence, they also address the importance of protecting the hardware in order for a society to function in the event of a crisis. In addition, the importance of artificial intelligence (AI) to the total defence is highlighted, as well as how faked news images can undermine the will to defend Sweden.

Chapter 14 is also this year's special chapter, where another agency contributes to this report. In this Strategic Outlook, the Swedish Fortifications Agency has been invited to give its perspective on how Sweden can store and protect information in secure environments, such as in underground facilities. The

chapter makes it clear that such protection cannot be built in the blink of an eye.

Finally, Chapter 15 shows how FOI can contribute to a strengthened total defence by introducing a new knowledge model. Following the decision to resume total defence planning, parts of FOI's activities have been gradually adapted to meet the knowledge requirements of those that task the agency.

FOI' in-depth knowledge of and insight into both the civil and military elements of the total defence is one of its major strengths. This understanding provides a unique opportunity to contribute to the development of many different parts of the total defence. Identifying important areas, together with the Swedish Armed Forces and the Swedish Ministry of Defence and other important agencies, is crucial for making FOI's research relevant for the total defence in the years ahead. This is something that benefits both the total defence and a safe and secure Sweden.

The report has involved authors from all of FOI's research departments. In addition to thanking the authors, I would also like to thank the editors and their immense contribution that has made our eighth Strategic Outlook possible.

Stockholm, May 2019

Anna-Lena Österborg
Acting Director-General
FOI - the Swedish Defence Research Agency

1. Sweden's total defence – global trends and new challenges

Samuel Bergenwall and Carina Gunnarson

Sweden's defence and security policy is facing major challenges over the next five to ten years. The improved security situation that came about after the end of the Cold War has come to an end. While the world's social and economic development remains positive, there are trends indicating greater instability and uncertainty both globally and in Sweden's immediate neighbourhood. This negative global development places greater demands on Sweden's military and civil defences. Sweden's new total defence needs to adapt if it is to be able to handle new challenges in a changing world.

The global security situation has deteriorated

Tensions have increased in the Baltic Sea region following Russia's illegal annexation of Crimea and ongoing aggression against Ukraine. The United Kingdom's process of withdrawal from the EU and the Trump administration's security policy have contributed to the unpredictability of developments in security policy both in Europe and elsewhere. The situation in the Middle East and North Africa, on the southern fringes of the EU, remains unstable and is affecting European policies and cohesion.

There are also growing tensions in Asia, a region that has an increasingly important part to play in the global economy and security. Increased tensions and conflicts outside Europe involving countries such as the US, China and Russia are affecting multilateral organisations like the EU, NATO and the UN. The repercussions of these are felt in Sweden and its immediate neighbourhood, too. China's military rearmament and desire for greater political influence both regionally and globally have security policy implications for Sweden as well.

The rules-based world order, democracy and globalisation are facing challenges

The gradual shift in the balance of political power from the West to Asia has brought with it major challenges to international rules and standards. The dominant role of the US in the international system that was established after the Second World War and reinforced after the end of the Cold War is undergoing a process of change. There is growing uncertainty about the global role of the US, its support for the rules-based world order and its continued

commitment to European security. At the same time, emerging regional and global powers and non-state actors are attempting to challenge international standards and undermine the Western-led, rules-based world order. Great powers are once again trying to establish spheres of influence, while established multilateral institutions are becoming weaker.

At the same time, democracy has been weakening over the last decade, with declining respect for civil rights and the rule of law. This trend is apparent in the vast majority of regions around the world, including Europe, resulting in increased risks to security. One source of concern is the fact that several of the biggest states in the world, including Russia and China, are becoming increasingly authoritarian. In a number of countries, democracy is being challenged by populist forces that are critical of globalisation and multilateral organisations. Although international trade remains extensive, there is a clear trend towards isolationism and the restoration of national sovereignty over political and economic decisions.

As a small state dependent on exports, Sweden benefits from international trade, a democratic environment, strong multilateral institutions and a rules-based order. These values are under threat from economic isolationism, authoritarian regimes, the undermining of international law by some states and further weakening of the current world order.

These developments, particularly in Sweden's immediate neighbourhood, are making more stringent demands of the total defence. Sweden is largely dependent on effective, open and free markets for its imports of food and strategic raw materials. The challenges facing international trade mean that the total defence needs to increase its level of preparedness, enabling it to cope with situations in which Swedish energy and food supplies are under threat.

The nature of conflicts is changing

The impact of hybrid warfare, as it is known, in the grey zone between peace and war represents a growing challenge. As a result, some states are using non-military force – information warfare, cyberattacks and economic pressure, for example – to influence politics, policies and societies of other countries. Open military conflicts may potentially be supplemented by attacks on civilian infrastructure and decision-makers, for example, or by distributing misinformation. Cyberspace is an increasingly important arena for conflicts. This means that influence operations

– for instance – can be executed from farther away than ever before and identification of aggressors is a difficult task, making deterrence and countermeasures more of a problematic issue.

Technological development and digitalisation have brought about many advantages but resulted in new vulnerabilities as well. State and non-state actors have acquired new ways of influencing societies without needing to resort to traditional military force. This is why preparedness among all authorities and a reinforced total defence are becoming increasingly important.

The more prominent role of nuclear weapons

Russia's rhetoric and the modernisation of its nuclear arsenal are causing major uncertainty in Sweden's immediate neighbourhood. There has been an increase in the risk of nuclear weapons being used in the immediate neighbourhood. Hence, total defence needs to relate to a world in which the significance of nuclear weapons is becoming increasingly prominent.

Western powers have begun modernising their nuclear arsenals. It is not clear whether Russia and the US will reach consensus and renew existing agreements on arms control. China, India and Pakistan are also continuing to develop and expand their nuclear arsenals. The conflicts relating to the nuclear programmes of Iran and North Korea remain unresolved. There is also a risk of nuclear weapon technology and weapons of mass destruction of other types spreading to more states, but also to non-state actors.

Growing impact of climate change on security policy

An increase in global average temperature has many consequences: increased sea levels, extreme weather, impact on agriculture, fires, water shortages, flooding and migration. There are potential risks of instability and conflict for resources due to climate change, in combination with weak institutional capacity in vulnerable states.

The consequences of climate change on security will be significant, particularly in the Middle East, Africa and South Asia. Climate change is also affecting Sweden's immediate neighbourhood. Deglaciation in the Arctic is opening up new offshore transport routes and facilitating new recovery of energy and minerals. However, this development is also reinforcing rivalries and conflicts of interest between states in and around the Arctic, in particular between China, the US and Russia. Climate change is also impacting Sweden directly. There is a greater risk of fires, for instance, which places demands on the crisis management system.

Major implications due to rapid technological development

Rapid advancements are taking place in fields such as information technology, artificial intelligence and robotics, which may have major economic and military implications and lead to a shift in the global balance of power. Improved accessibility and distribution of new technology means that states and non-state actors are able to access civilian and military technology that was previously exclusive to the West. China, for example, has a long-term plan to become a world leader in the field of artificial intelligence.

New technologies are providing more opportunities for states to operate in the grey zone between war and peace without having to cross the threshold of armed attack. Given this fact, it is important for Sweden to monitor technological developments closely and ensure that its total defence is updated regularly so that new threats and challenges can be handled.

World military expenditure on the increase

Global military expenditure is currently at its highest level since the end of the Cold War. This is mainly due to the massive increase in military expenditure in China, Russia, India and Saudi Arabia over the past decade. The percentage of global military expenditure by democratic and Western states – particularly countries in Western Europe – has declined over the same period. States such as China and India are likely to continue increasing their percentage of total global military expenditure. At present, the military expenditure of the US corresponds to just over a third of the total expenditure of the world.

Military expenditure in Europe is once more on the increase due to the behaviour of Russia. Although the US has increased its military presence in Europe, there is now greater awareness among European states of the need to take more responsibility for European defence and security.

The ratio of Sweden's military expenditure to GDP has been falling since the end of the Cold War and is currently equivalent to one per cent of its GDP. There is currently a need to reinforce both the civil and military defence postures if the targets outlined in the 2015 Defence Act are to be met.

Sweden faces important security policy decisions

The development of Sweden's total defence is once again of renewed relevance due to the deteriorating security situation in the world. The planning of a new total defence is influenced by the development of Sweden's relations with the EU and NATO and how these organisations adapt to the new global dynamics.

The organisation of total defence is also affected by Sweden's cooperation within the Nordic region and with the Baltic States, as well as its cooperation with strategically important countries such as the US and the United Kingdom.

While the old total defence was primarily organised to confront and deal with military armed attacks, the modern total defence must be prepared to face a significantly broader threat scenario in which attackers cannot always be identified. The total defence needs greater resilience, adaptability and capacity if it is to be able to cope with the challenges presented by technological development and the changing security political dynamics.

To summarise: as a globalised state, Sweden must prepare for a more uncertain world and develop its capability to defend Swedish territory, safeguard the security of society and protect its democracy from hostile external influences. These challenges place important demands on Sweden's total defence concept.

2. Prerequisites for the total defence then and now

Maria Lignell Jakobsson

Total defence planning was resumed in 2015. The last time active work was carried out in this area was during the 1990s. Since then, Sweden has become an EU member, the Swedish Armed Forces has been radically transformed, technological development has accelerated and Sweden has been opened to an increasingly changing world. At the same time, we have the same needs as then for basic security, including the supply of essential goods and services. A new total defence concept needs to be informed by previous experience, but above all to be built on new capabilities and knowledge based on current conditions. This chapter highlights some differences and similarities between conditions at the present time and at the end of the period when active total defence planning was last carried out, i.e. the 1990s.

The time of the great decommissioning

During the 1990s, the total defence was transformed, from the Cold War's nuclear threat and invasion defence into a defence against a strategic assault. The then new focus was on the risk of a military attack with minimal warning, with limited forces of high quality, aimed at controlling functions vital for the country's total defence. A transition was initiated away from a total defence that involved a large part of the population, by means of conscription, civil defence, voluntary organisations, home guard and so-called war-critical companies (companies important for the war effort). It also included extensive stockpiling of fuel and food in particular. The development of a smaller but more appropriate total defence had started.

There was an overall need for change, and work began on a large scale to achieve this. The existing methods for developing operational capability were gradually changed from a focus on resources, equipment and contingency plans. Amongst other things, the transformation was aimed at increasing quality at the expense of quantity. In the mid-1990s, the Swedish Armed Forces was formed after a merger between a large number of separate authorities. In addition to this reorganisation, cost cuts in the total defence was initiated. The overall result was an extensive disbanding of military units and resources for civil defence.

The concept of a 'grey zone' was already used in the 1990s, at that time to illustrate the lack of clarity over what conditions prevailed. Then, as now, it was not clearly defined. Some parameters were

the preparedness level i.e. the threat scale of peace-crisis-war; *total defence actors*, both military and civilian, both public and private; and *antagonists*, i.e. enemies that could be a nation, organisation or individual. Dependencies between the Swedish Armed Forces and various civilian functions were emphasised, and a need for better coordination therefore started to become clear.

In the 1990s, there was already a long tradition and a lot of accumulated experience in the total defence sector, since so many individuals had been involved in total defence and many still had a role in the system. Many people with a military background also worked within the civilian part of total defence. In addition to experience and broad knowledge, there were networks and structures for command and control, even at a higher regional level. The total defence was divided into different areas with designated responsible authorities and thus a clear structure of responsibility.

With its entry into the EU in 1995, Sweden began to open up to cooperation in many areas, not least in the defence sector. Sweden also phased out a food policy based on a high level of self-sufficiency. Entry into the EU, in combination with globalisation, changed the basic conditions for both Swedish security policy and total defence.

Other significant trends during this period included market liberalisation and internationalised trade flows, as well as a reduction of the state's role in society. Amongst other things, this led to a transition from public to private ownership in many sectors of society. Today, this places new demands on clarity and clarification of any preparedness requirements in procurement – especially with subcontractors at multiple levels.

During the period from the turn of the millennium to 2015, the focus, on the military side, shifted from total defence to international operations and to the crisis management system on the civil side. The disbanding of units and total defence resources continued. Responsibility for the total defence was divided between two ministries, and today there is no longer any special organisation or any special resources for a heightened state of alert and war. Knowledge about how to plan for war has been forgotten.

Changed and new conditions

Since the end of the 1990s, not only has the outside world changed, but so have Sweden and Swedish defence. An important detail in this context is that considerably fewer people have contact with total defence-related activities today. Conscription was mothballed for a number of years and fewer people are currently involved in voluntary defence organisations. Citizens are not involved to the

same extent as before, and therefore knowledge is also lower in large parts of the population. A generational change has taken place in many authorities, and few of their employees today have first-hand experience of total defence planning.

The demand for development of and knowledge about total defence has grown with the need to be able to handle changed or new conditions. One example is the changes that have taken place in information technology and (social) media, which place completely different demands on information security in particular, and on security protection activities in general. A clear structure also needs to be developed for command and control of the total defence with both geographical and functional divisions, i.e. which roles the authorities and other actors occupy. The arenas for warfare have extended beyond the traditional land, sea and air into space and cyberspace. This calls for new knowledge and planning. There is also a need to clarify concepts based on the new conditions. The fact that these new arenas exist, and that an opponent can use means of attack other than traditional military action, places new demands on the development of capabilities within the civil defence.

International cooperation takes place in many areas and in a completely different way today, in particular within the EU and the Nordic countries, and support is provided and received in different ways. One example is the aviation resources that Sweden borrowed for firefighting during the extensive forest fires in the summers of 2014 and 2018. Within the EU, the development of defence cooperation between governments is also underway through the Permanent Structured Cooperation (PESCO) in which Sweden participates.

Timeless needs and requirements

Although the conditions of the 1990s differ to the present day in various respects, there are also common denominators. Society`s need for functioning services and basic security remains. As was the case then, the focus is on increasing operational defence capability, the individual's ability to survive, and the robustness of important societal functions. These can be considered as basic starting points for total defence concepts regardless of the time we live in. There are a number of generic capabilities that need to be developed and which will always be needed based on these common denominators. These include energy and food supply, healthcare, communication and transport.

The threat scenario is now characterised by great uncertainty and the importance of being able to handle a grey zone situation with

elements of surprise. The concepts of hybrid warfare and non-linear warfare are sometimes used to describe these conditions.

Common to the 1990s and the present day is the need for a joint overall priority regarding both resource building and the utilisation of such resources in order to strengthen the country's overall defence capability. The need to clarify the dependencies between different societal functions remains, as well as the need to plan, train and practise in order to be able to provide adequate mutual support (between the military and civil defence).

The road to a new total defence

The Defence Act of 2015 initiated a change when a military threat was emphasised again. New funds were provided and, amongst other things, the defence of Gotland was emphasised. Many activities are now underway in the total defence. For example, total defence planning has been restarted, conscription has been reinstated, resource build-up has been started, military defence has been reorganised and governmental inquiries have been initiated.

Above all, there is a significant need to build new knowledge about total defence, but also to seek knowledge from the past. One way of doing this is by consulting retired key personnel with relevant experience who can provide support in understanding the system. Both the Military Archives and FOI's archives have become sources for recalling knowledge. It is important to learn lessons from the work that was carried out to modernise the total defence in the 1990s, and at the same time to adapt capability building according to current and future conditions. Problems may be encountered when attempting to strengthen capability within vital parts of the total defence without first having thoroughly investigated the current conditions, and thereby risking developing old solutions, that do not need to be recreated or which are obsolete. Another risk is sub-optimisation if different needs are not weighed against each other as part of an overall societal balance.

However, the major challenge is to be able to provide simple and comprehensible answers to authorities and other actors, which can be used for managing and planning the total defence, an area where complexity is extensive and where there is a high degree of uncertainty. As civil defence consists of all relevant authorities, organisations and companies, it has been proven difficult to develop relevant plans and policies, as well as follow-up and control, for civil defence. There is therefore a need for development with regard to governance, financing and follow-up in order to manage the range of actors on the civil side.

A new total defence concept needs benign conditions to grow. This requires knowledge in many areas, some of them new; analysis capacity; interoperability; and not least time to think.

3. No fast track towards civil defence

Carl Denward

The network of actors who today constitute the Swedish crisis management system and civil defence can be referred to simply as the Swedish preparedness system. This system is about to embark upon a lengthy development towards a new civil defence that makes up one of the two parts of the Swedish total defence concept. The task of rebuilding the total defence will be taken on in collaboration with the Swedish Armed Forces. However, there are signs that the civil defence development process is at risk of being affected by a number of difficulties.

The historical context of the peacetime crisis management system

The new civil defence has strong ties to the existing peacetime crisis management system, which was created in the early 2000s in the wake of a Swedish Government Official Report called 'the Vulnerability and Security Study' (*Sårbarhets- och säkerhetsutredningen*). This report marked the end of the historical civil defence, which had been based on a Cold War context, and introduced a crisis management system for peacetime purposes. Aside from the current crisis management system and the legacy of the old civil defence, a new civil defence needs to take a number of conditions into account. Examples include:

Pluralism. The contemporary authority landscape is pluralistic, including a growing number of specialised authorities. Furthermore, many societal functions that traditionally operated within the public domain are now run by the private sector . Private ownership has in turn become more complex, since some companies that perform vital societal functions have foreign owners and are governed by principles that are not necessarily aligned with the interests of the Swedish preparedness system.

Technological development and emergence of vulnerabilities. Today, our modern society relies increasingly on critical technical and socio-technical systems. This is a favourable order of things during peacetime, but also constitutes potential vulnerabilities should society be subjected to intense pressure. One could argue that these vulnerabilities are greater for the part of the population residing in cities, as opposed to those in the countryside, who are somewhat less dependent on (or have

no access whatsoever to some of) the different kinds of services that society offers.

Grey zone and hybrid warfare. So-called hybrid warfare brings with it new ways to influence Sweden. This makes the challenges of a grey zone threat more relevant than ever. The grey zone threat concerns deniable attacks at levels below open armed conflict, in situations where there is neither peace nor discord. Regardless, this problem represents a number of new and old aspects that a total defence needs to take into account when it comes to capabilities, alongside those needed for conventional warfare.

Giving direction to governance

Actor pluralism lends complexity to activities such as governance, development of concrete capabilities, financing and follow-up measures. A possible solution includes tailoring actor-customised governance models in order for civil defence to gain input from the various actors in the preparedness system, such as municipalities, county administrative boards, county councils and central authorities. There is great demand for well thought-out governance efforts by the state – efforts which are associated with some complexity, as the preparedness issue is cross-sectoral and concerns several parts of society, while it rarely represents a core issue among actors who are obligated to participate.

In the context of governance, one can argue that the preparedness system is hampered by deficiency in the input parameters which preparedness actors need in order to be able to plan and develop civil defence. The governance directives regarding which parameters actors should take into account concerning scenarios of conventional warfare or grey zone threats are at best abstract and at worst ambiguous. It would be complicated for a single preparedness officer, for instance at a municipality or a central authority, to discern which capabilities his/her organisation is to bring to the table and how these are to interact with the rest of the preparedness system, based on the governance directives provided today.

The Swedish government's most recent Defence Bill that was passed in 2015, the total defence doctrine issued by the Swedish Civil Contingencies Agency (MSB) and the Swedish Armed Forces, and the cross-party Swedish Defence Commission's report 'Resilience' (*Motståndskraft*), all provide some indications of which capabilities are to be included in civil defence. However, there is a lack of a systematic and exhaustive approach defining which actors are expected to do what, and how the different aspects of civil defence are to be linked together in concrete terms.

The preparedness system also lacks a hierarchy of objectives which could be used to specify the three main objectives of civil defence: to safeguard the civilian population, to ensure societal basic functionality, and to support the Swedish Armed Forces. These three formulated objectives could be broken down into a number of desired capabilities, which can be taken on by the actors in the preparedness system in the form of concrete activities. This breakdown was, to an extent, carried out within the former civil defence during the 1990s.

Avoiding analysis traps and sub-optimal responsibility structures inherited from the crisis management system

Some difficulties remain in the legacy of the peacetime crisis management system created in the early 2000s. First, the system is characterised by some ambiguity regarding which actor is responsible for what and which role each actor is to fill. This ambiguity is manifested in part in the so-called preparedness 'cross-sectoral cooperation forums' and their relationship to the so-called 'sector responsibility' mechanism. These forums aim to promote collaboration among authorities, for example in the areas of chemical, biological, radiological and nuclear weapons (CBRN) or technical infrastructure. A focus on collaboration within the forums has rather become an objective in its own right rather than focusing on planning and coordination efforts aimed at achieving concrete capabilities.

Preparedness actors have recently started to recognise that the crisis management system's sector responsibility, i.e. the responsibility structure that is expected to guarantee the central authorities' participation in preparedness efforts, is in many respects too vague to have any real effect. A formal sector responsibility probably needs to be clarified for the cross-sectoral cooperation forums to function properly. Nevertheless, there has been some improvement in the energy and transport sectors, though the road to a functioning sector responsibility mechanism will be long and tedious. In this respect, it can be added that sector responsibility is a means, rather than an end – which is why preparedness objectives initially need to be formulated on a sector level.

Furthermore, the sectoral responsibility mechanism will have to be customised depending on which sector is concerned, as each individual sector system is characterised by its own conditions and actors.

Second, the crisis management system places a disproportionately large focus on risk analysis, which, in many cases, involves analysing risks and vulnerabilities already identified, while

working out solutions and measures is deprioritised. Some actors have been wholly or partially caught in this analysis trap, which is why it will be important in future for the state to request and disseminate smart preparedness solutions and measures, rather than updated risk and vulnerability data.

The government considers that civil defence should be based on crisis management, which is a sound approach to managing society's limited resources. Concurrently, it is important that the development of civil defence avoids reproducing the shortcomings of the crisis management system. One should also bear in mind that an evolving civil defence system can help the Swedish crisis management system to improve, in terms of capabilities.

Some questions to consider in the development of civil defence

All in all, the difficulties described above present a risk that a new civil defence may evolve in an unnecessarily chaotic and arbitrary manner. Such a development may cause separate actors to plan in separate directions, which might result in poor prospects for the system as a whole to work towards a common objective. This also complicates the potential for the actors to work together in a coordinated way, for instance in efforts aimed at creating interoperability between capabilities. A development of this kind involves a risk of wasting or misdirecting resources and development efforts being carried out in the wrong order, which may exert unnecessary stress on the motivation and drive of the personnel.

Considering the ambiguity in the current governance of the civil defence development process, preparedness actors such as authorities and municipalities are presented with a difficult task in determining their respective roles and core activities. In turn, the vagueness of governance might cause actors to focus on developing what could be called 'support capabilities' – for instance, conducting exercises, hierarchies of command and information security. With the exception of protecting information, which is vital in order to even start planning processes, the civil defence development could benefit from establishing a bottom-up perspective which places greater focus on actors' core capabilities – which comprise the very reason for the actors to participate in civil defence in the first place.

In conclusion, a few proposals are presented below, with the ambition of supporting the ongoing discussion about what contributes to the development of an appropriate civil defence.

Conduct development activities in the right order. The Swedish Civil Contingencies Agency (MSB) is currently assigned to develop a so-called set of starting points to support planning efforts among civil defence actors. These starting points should provide the basis for the formulation of capability-related objectives regarding both the traditional armed conflict and the grey zone ends of the threat spectrum. Efforts on formulating capability objectives should be carried out in consultation with actors in the civil defence system, in particular the so-called sector-responsible authorities. Furthermore, we need to determine which actors should contribute with which capabilities and how these can be translated into concrete activities. This needs to be supported by governance, financing, and necessary changes in legislation.

Bring threat spectrum professionals together with capability development professionals. FOI's predecessor, the National Defence Research Institute (FOA), had already stated in the 1990s that professionals who work to create capabilities among civil defence actors need to be brought together with professionals who understand the antagonistic threat, in order to facilitate an apt capability development process. The reason for this is that knowledge of threats and knowledge of the activities of specific organisations is rarely found in the mind of one and the same person.

Imbue the civil defence development process with a capability balance. Efforts towards a well-thought-out development of civil defence need to aim at creating a balance between different capabilities. This needs to be done in two contexts. The first is represented by an internal capability balance within the civil defence: we need a certain amount of qualities and quantities of capabilities in the civil defence system. For instance, civil defence does not only need a working war-time hospital preparedness, but also a robustness in the power and telecommunications sectors. The second context represents a balance within the total defence system - between civil and military capabilities. A strong military deterrence is desirable, but should be weighed against a corresponding civil defence threshold. A weak civil defence deterrence is undesirable, as it might invite a potential aggressor to ignore conventional means and strike from within the grey zone spectrum.

Avoid allowing time constraints to limit the development. A proper civil defence comprises a comprehensive societal project that will take time to implement. A long-term development plan should be drawn up and resources allocated only when

there is an assessment of what should be achieved and how different activities could be linked together.

Remember that we still need a crisis management system. Consideration should be given to how potential civil defence capabilities can also be used for the benefit of managing peacetime crisis situations. This could affect how certain capabilities are designed in the first place in order to allow a dual use practice. In addition, lessons should be learned from our soon to be twenty-year-old crisis management system regarding which aspects have worked well, and which aspects have underperformed. Finally, it is important to confront the occasional misconception that we must make a hard trade-off between a civil defence and a peacetime crisis management system: in terms of capabilities, I would argue that the latter can benefit greatly from investments in the former.

Study the interfaces between the sectoral responsibility and geographical area responsibility. The crisis management system suffers from ambiguity in the interconnection between the actors responsible for geographical areas (e.g. municipalities, county administrative boards) and those responsible for the different so-called sectors (e.g. with responsibility for electricity, food or financial systems). In this respect, the 'civilian commanders' of the Cold War civil defence represented an important function. The commanders acted as contact interfaces, on the one hand between the civil defence system and its military counterpart, and on the other between the geographical area actors the sectoral/central authorities. Is a corresponding interface desirable in a contemporary context, and should it be restored?

Ultimately, a lot depends on how the national political level, the government offices and the Swedish Contingencies Agency (MSB) decide to mount a comprehensive approach. In what place do we want to find ourselves in five years, and what kind of civil defence is desirable? Once a comprehensive set of capability objectives is established, it is high time to compile a strategic governance package to enable civil defence actors to develop the right capabilities. The recently announced and initiated Swedish Government Official Investigations are instrumental in laying the groundwork for these governance efforts.

4. Creating commitment and capability for total defence

Bengt Johansson

Building a resilient total defence requires both will and capability. Communicated threat scenarios need to be perceived as relevant, and trust in society and its institutions must be preserved in order to create a sufficient impetus to act. Information and requests coming from public authorities and municipalities need to be perceived as reasonable. Stressing the importance of general robustness in society and the benefits of this in peace, grey zone and war can increase the motivation of individuals, authorities and companies to contribute to the work on total defence.

Total defence calls for new priorities

Strengthening the total defence calls for new priorities. Increased efforts in this area may mean that other things must be ignored. Companies are expected to participate in the planning process, which is not normally part of their core business. Citizens are expected to cope for a relatively long time in difficult conditions with only limited public support. Finally, the prioritisation of robust systems often conflicts with the efficiency aspirations that characterise modern society.

In order to create a commitment among organisations and individuals to set aside time and resources for preparations, the threat scenarios used need to be perceived as sufficiently relevant. However, that the threat scenarios are important and useful does not create sufficient conditions to create a willingness to act. What is also required is a belief that defence is meaningful and that what is to be protected is worth defending.

As the sociologist Ulrich Beck points out, for example, threat scenarios are things that are created. Threat scenarios may be challenged in terms of their content, how they are to be interpreted, their relevance and whose interests they reflect. The threat scenario described by the Swedish Defence Commission from this perspective can be seen as a jointly created scenario, anchored in democratic institutions. This does not prevent the scenario from being discussed and problematised in different ways; such a problematisation is part of a democratic society. However, discussions and debates can complicate the governance of the total defence.

Identifying threat scenarios

The end of the Cold War saw the rise of an expectation of peaceful coexistence in the region. The notion of a war in Sweden or in the wider region was not perceived as realistic. Society became used to calm and peaceful conditions, and vital societal systems were dimensioned accordingly.

An important challenge for the planning of the civilian part of total defence (civil defence) is therefore to describe what war, war-like conditions and grey zone threats mean, and to transmit these accounts, so-called narratives, to various societal actors and the public. Examples of such narratives are the five scenarios that FOI has produced on behalf of the Swedish Civil Contingencies Agency (MSB). The scenarios are intended for use by actors in society, such as governmental authorities, in the planning of civil defence. Another example is the Swedish Defence Commission's description of the security situation and its importance. A greater awareness of the risks of psychological warfare, of the disruption of electoral processes, and of a perceived increased risk of armed conflicts in the wider region has also been fostered through reporting by governmental authorities and the media.

Interpreting threat scenarios

Threat scenarios can be interpreted in different ways. They may be challenged with regard to their relevance or weighed against other threats. As mentioned above, a threat in this context is something that is designed, and it is legitimate in a democratic society to insist on an interpretation that differs from those presented by the government and other actors.

One complication is that there is a risk that hostile actors will also question the accuracy and relevance of threat scenarios. Criticism of the threat scenario can be communicated directly or indirectly via organisations, individuals or fictitious accounts on social media. It will therefore be important for public authorities and municipalities that there is trust in society and its institutions, in order to be able to assert with credibility the legitimacy of the particular threat scenario that the authorities want to present.

Acting according to threat scenarios – to want and be able to

Even if there is an awareness of a threat scenario and it is interpreted as being relevant, it may inspire different types of behaviour. To act according to a threat scenario, in the way the state desires, requires a willingness to act, often referred to as the will to defend; and in addition, competence and resources.

The will to defend is not an unambiguous concept and can be interpreted in many different ways. At the future planning stage

of total defence, it may mean that it is considered reasonable to prioritise defence instead of focusing efforts on achieving other non-defence policy objectives. During an ongoing conflict, it may mean the will not to surrender, to personally fight against an ongoing aggression, etc. By using the concept of the will to resist in a conflict, it is possible to distinguish between the will to defend before and during a conflict (see figure below).

	Before	**During**
Activity	Planning	Management
Reality to relate to	Threat scenario What might happen?	Operating picture What is happening?
Will to defend and will to resist	Will to defend • Acceptance of prioritising preparedness measures • Participation in voluntary organisations • Build-up of own personal preparedness	Will to resist • Support to not surrender • Willingness to personally fight ongoing agression • Willingness to participate in voluntary rescue and repair efforts

Figure 1. Conceptual figure illustrating similarities and differences between total defence before and during an attack. The figure is a policy sketch and there is not always a clearly defined boundary between 'before' and 'during', which is one of the challenges presented by attacks in the grey zone.

For the individual, the will to defend may mean accepting making his/her own sacrifices in terms of time, money and/or convenience in order to build defence readiness. It may also involve citizens accepting restrictions on their own freedom in the form of, for example, military service. For society as a whole, it may be a question of whether more resources should be allocated to total defence, possibly at the expense of resolving other societal problems, developing other social infrastructure, or reducing taxes.

The priorities of different actors affect the will to act

Public sector actors, such as governmental authorities, county councils and municipalities, work towards a wide range of societal objectives in their respective policy areas, where many issues are of equal importance. The regulations that govern these activities are vague in many cases, and their objectives are open to interpretation. This means that, to a large extent, the various actors have to weigh up themselves how resources should be prioritised.

This means that priorities in terms of societal objectives may differ between authorities, municipalities and regions, depending on which areas and which threats are considered the most important. This is understandable, since the conditions for action differ greatly. Perspectives on the relevance of the threat scenario may also differ depending on understanding of the outside world by individuals or groups of officials and other actors.

One way the government and parliament might deal with this would be to prioritise more clearly between different societal objectives. So far, this has not been done to any great extent, and indeed it may not be possible. This applies in particular in the case of overall objectives that are often not sufficiently well-defined in order to be able to clearly determine whether and when they have been achieved. The prioritisation of such an objective could, in theory, lead to no action being taken to achieve other objectives, which would in all likelihood eventually be perceived as unreasonable. There will therefore need to be a continued compromise between different objectives.

The state can also give direction by means of targeted financial support, something that has been common in the crisis management system, but this support is generally insufficient to cover all needs. So the question of prioritising between different societal objectives is likely to largely concern the role of individual actors in the future as well. How important total defence is assessed to be in comparison with other activities in society, and what should be prioritised within the total defence, will likely differ between these different actors.

The business sector is an important actor in civil defence, although the main task of companies is to produce goods and services in order to generate profits for the owners; contributing to the public interest is not a key priority. Nevertheless, companies may have a self-interest in contributing to civil defence. For example, participation may strengthen a company's brand and thereby indirectly contribute positively to the financial result. Furthermore, companies consist of individuals, who can exert their influence on the business to take greater account of the interests of the total defence.

Even if there is a willingness in society to act, resources and skills are required for this. Financial resources and personnel will need to be allocated. Employees who are needed in total defence will require training, and this will take time. Priorities will have to be defined and it will not be possible to implement these solely at central level.

Is a common understanding of a threat scenario possible?

There is a need for threat scenarios to be addressed in order to motivate actors to allocate time and resources to planning and action. A common operating picture is highlighted by many sources as being central to the efficient management of an ongoing event. There are also major advantages to an increased common consensus in cross-sectoral planning between different sectors, such as energy and transport. However, the question concerns what degree of consensus can be reached between a broad set of actors with different interests and priorities. Having access to the same threat scenarios can be valuable, but it does not necessarily mean that actors share the same understanding of the threat scenario.

Even if it is possible to create narratives, such as FOI's scenarios, these need to be interpreted in the different contexts of the actors concerned. For example, it is not self-evident that the same scenario will be perceived to be best for planning in all sectors; in some cases, the scenario that is most relevant may be war, in others the grey zone.

As mentioned above, the various sectors are fully occupied with contributing to different types of societal objectives, and it is in relation to this that their prioritisation of total defence must be understood. It will likely be difficult to reach full agreement on a common threat scenario. However, this does not mean that the work on building civil defence needs to come to a standstill.

A robust society for a broad scale of threats

One way of avoiding dependence on a general acceptance of a particular threat scenario, and also motivating work when acceptance is low, is to shift the focus to building a robust society that can be resilient according to a broad scale of threats. This may be a question of creating a food supply that is resistant to disruption, no matter the cause. It could also be a question of the capability to handle disinformation or cyberattacks, regardless of whether the perpetrator is a state actor or a group of activists. Most importantly, it may be necessary to work to maintain confidence in democratic institutions. These form the basis for all the measures that the state expects individuals, organisations, companies and authorities to perceive as legitimate.

Such a perspective in civil defence planning is likely to help different actors agree on the value of activities that make society more robust, without needing to embrace the same specific threat

scenario. In this way, there would also be greater opportunities for building coalitions of stakeholders in order to implement measures. A concrete focus on robustness may also be advantageous with regard to the ambiguity of the grey zone threat, where it may be unclear whether events are the result of hostile attacks and, if so, what intentions the antagonists may have.

This does not mean that all aspects of civil defence can be dealt with in this way. There are several parts of civil defence that are not directly linked to the building of a general robustness. This applies to the support from society for the Swedish Armed Forces, for example.

Basic prerequisites for success in total defence

Relevant threat scenarios and clear government direction are both needed to build civil defence. However, it is important to be aware that objectives and threat scenarios are emotively charged and that motivation and willingness to work from them are not foregone conclusions. Changing the perspectives of citizens, the business sector, authorities and other actors, so that total defence is given greater priority in their daily activities, is not achieved overnight. If synergies can be found between the requirements of total defence and the other interests of different actors, it may strengthen the willingness to take total defence into account in their activities. For these attempts to bear fruit requires confidence in the institutions of society. For this reason, information and requests presented by the authorities must be perceived as reasonable by the population.

5. Total defence, information sharing and new interfaces

Ann Ödlund and Matilda Olsson

Serious shortcomings in information sharing between the actors in the total defence can lead to the creation of isolated 'islands' in different parts of the total defence and in different geographical areas, instead of coherent planning and coordination. If information sharing does not work, it will be difficult to answer certain questions from a national perspective, such as 'What do we have?', 'What can we do?' and 'How do we prioritise?' - regardless of whether it concerns planning or action in an actual crisis. Well-functioning information sharing within and between the actors in the total defence is a prerequisite for total defence planning and civil-military coordination.

Information sharing: The glue in the total defence

To be able to plan and make informed decisions, decision makers at different levels are dependent on both specific information and common operating pictures that provide an overview of a particular area, situation or sequence of events. Operating pictures are used in the crisis management system and in military defence, and are based on information gathering, analysis of information, compilations and intelligence. Operating pictures are essentially developed specifically by authorities and other actors in order to understand and obtain an overview of an unfolding crisis or event. This is in order to notify other authorities of the information requested or to provide a basis for common operating pictures at higher levels. Operating pictures are context dependent. Recognised Maritime Picture (RMP) is one such example.

Authorities with specific responsibilities in the crisis management system have an obligation to share information and operating pictures with each other. In turn, these obligations lead to the formation of a network in which information can be shared between actors and administrative or hierarchical levels in peacetime as well as in war. In the case of information for the government in peacetime, each authority, upon request from the Government Offices or the Swedish Civil Contingencies Agency (MSB), must provide the information that is needed for common operating pictures. During a heightened state of alert, the authorities must keep the government informed about the current situation and the development of events within each of their areas of responsibility, as well as about action taken and planned. The Swedish Armed Forces must also receive the data that it needs from the authorities, such as the National Board of Health and

Welfare and the Swedish Energy Agency, as well as from other defence authorities, such as the Swedish Defence Materiel Administration and the National Defence Radio Establishment, in order to be able to fulfil its obligation to provide information to the government in the event of a heightened state of alert.

Information sharing and common operating pictures processing can be problematic even in the context of peacetime, as observed during the storms Gudrun (2005) and Per (2007), the forest fire in Västmanland (2014), the terrorist attack on Drottninggatan on 7 April 2017, and the forest fires in the summer of 2018. The problems were technical, due to shortcomings in procedures and uncertainties over how information should be shared within organisations and between actors.

The perspectives of grey zone and heightened state of alert place additional demands on actors. In the case of grey zone, there is considerable uncertainty as to whether disruptions or other events are caused by a foreign power, terrorism, sabotage or accident. This uncertainty implies that those responsible for information sharing and for compiling and interpreting common operating pictures are faced with situations that are difficult to assess, where misjudgement risks giving a potential opponent an advantage. Even in the event of a heightened state of alert, where there is a known opponent in the form of a foreign power, uncertainty will remain for decision makers. In addition, there is the case of a war situation or threat of war as a basis for decision making, which means that focus and priorities shift from peacetime crisis management to an activation of the total defence. Information sharing both in a grey zone and during a heightened state of alert, as well as in the transition from peacetime to war, needs to be planned and practised.

What is normal, what is different – and for whom?

In terms of the future conflict environment, an Armed Forces long-term perspective study (2016-2018) states that the year 2035 will encompass a wide range of threats. These hostile activities will include significant elements of non-linear warfare, where the boundary between peacetime and war is blurred and where cyber and influence operations may be included. In the grey zone, attacks need to be detected at an early stage, which in turn requires an overview of both civil and military incidents. The question is, firstly, over which actors should collect such information and compile it; and secondly, how it should be communicated. In the grey zone, it is perhaps primarily a question of the possibility of early warning and the detection of hidden attacks. The study of anomalies, i.e. significant changes in the normal situation, is fundamental here. Intelligence and knowledge about the normal

picture in different areas are therefore central to being able to assess events, to create an accurate basis for decision making and to take the most appropriate action. An additional question will be over who has the skills and resources to assess and communicate what is normal in different areas.

Much has changed in recent years when it comes to who owns or operates vital societal functions and critical infrastructure. Skills have been transferred from the public sector to the private sector and there are many new entrants. A clear example of where such a transfer has taken place is in the field of telecommunications. This development implies the need for a fundamental analysis regarding which areas and actors are relevant to the total defence in today's context. In other words, there is a need to take stock of which actors have the knowledge and thereby the opportunity to communicate information about what is normal and what deviates from a total defence perspective.

Aside from the particular characteristics of the grey zone, there are two factors that may potentially complicate information sharing. One is private ownership, which may create commercial barriers to sharing certain information, for example. The other concerns the need to maintain confidentiality in the distribution of information. Information sharing and coordination take place in the interfaces within and between authorities and actors. Research has shown that there are limitations in national conditions for sharing confidential information, such as between intelligence and security services and the broad circle of authorities responsible for emergency preparedness, for example. In this case, there are shortcomings in the technical systems for information transfer, cultural differences, limited resources, ill-defined mandates, as well as a lack of a clear boundary between the intelligence system and other authorities. Barriers and lack of trust between authorities or, in this case, sectors are examples of some of the problems.

Building new and changing old

An adequate function for sharing information and processing operating pictures is important for decision making in peacetime, grey zone and war, and its inclusion in the design of the total defence should therefore be ensured. The civil-military interface is central to everything from planning and supporting mobilisation, the supply of essentials such as food, fuel, and electricity, to healthcare and transport. An analysis is required of how civil-military coordination should be directed strategically, effected between central and regional levels, and realised between the Swedish Armed Forces and various civil actors. There is a need to

organise a total defence that can provide the conditions for this to be possible.

On the basis of the need for efficient structures for the total defence, the government issued a directive in 2018 for an inquiry into roles, mandates and coordination within civil defence, in order to create clearer conditions of responsibility. This inquiry will analyse and propose a structure for civil defence at central, regional and local level. According to the directive, the proposals should be based on the Swedish Defence Commission's report *Resilience* from 2017, which, amongst other things, proposes a division of governmental authorities into societal sectors, each with a sector-responsible authority. This and other forthcoming inquiries are likely to lead to new responsibility relationships and interfaces between actors, both civil-civil and civil-military. Building new means a chance to design the structures and the allocation of responsibilities according to the needs that exist within the total defence. All in all, the total defence is now being given opportunities for strengthening and improvement, which include not least a basic capability for sharing information.

Functioning information sharing is in everyone's interest

Common operating pictures are created through the compilation of information based on a specific purpose in a particular context, and constitute planning or decision data for both long-term deliberations and operational decisions. If actors lack relevant organisational structures, technology, training and understanding of the purpose and of their own role, information sharing risks being deprioritised. In turn, this may result in important information being omitted from planning or decision data. If the obligation to share information to meet a particular need is one side of the coin, the right to access information represents the other. One side of the coin cannot work without the other. The right to information is discussed less often than is the obligation to share it. The ability to handle confidentiality, cultural differences and a lack of understanding of different needs can constitute barriers.

It should be in everyone's interest to create the best possible conditions for decision makers to carry out their duties, both in planning and in operations. Each actor taking responsibility for their part in a chain of information sharing can ultimately determine what decisions are made. In a situation where time is scarce and the pressure great, decision makers need quick access to relevant information. For information sharing to work effectively in crisis and in war, functioning structures for both peacetime crises and a heightened state of alert must be in place. The design of these structures needs to be preceded by analyses and planning

concerning similarities and differences between peacetime and wartime needs. Ultimately, this is a balancing act between the use of known peacetime procedures and structures and a transition to an organisation adapted to the requirements of total defence.

Over the past few years, the total defence concept has changed from being a largely unwelcome guest, both in the crisis management system and in the defence policy arena, to becoming an increasingly central activity whose presence cannot be neglected. Today, there is a greater interest in and commitment to total defence issues, politically as well as among authorities and other actors. This may mean the renewal and improvement of the total defence, where the possibility of information sharing between authorities and private actors would be high on the agenda.

6. Sharing sensor data improves management of crises, terrorism and heightened state of alert

Maria Andersson, David Lindgren, Peter Nilsson, Åsa Berglund and Ola Svenonius[1]

In addition to the worsening international security situation, Sweden is at risk of terrorist attacks and an increase in serious crime. Total defence capabilities and crisis management need to be strengthened. Inter-authority cooperation and cooperation with rescue services and the Armed Forces regarding technical sensors and sensor data can contribute to strengthened total defence capabilities and crisis management. However, to accomplish this, the procedures of the authorities need to change.

Strengthening total defence through cooperation

The terrorist attack on Drottninggatan, Stockholm, in 2017, and the forest fires in northern Sweden of 2018, are examples of serious incidents where it became evident that inter-authority cooperation, between various government agencies, is of great importance to ensure an effective crisis response. For example, cooperation makes it possible to create a shared situation awareness, that is, a compilation of critical information provided by several authorities. Shared situation awareness enhances comprehension of the extent of a crisis.

Sensors and the data provided by sensors make important contributions to situation awareness. Surveillance cameras are an example of sensors frequently used by authorities. Sensor data include images captured by surveillance cameras and detection of objects, such as vehicles or number plates. Cameras are positioned around town squares, in underground stations and along roads and railways. In the event of a serious crisis, the rescue services, the Swedish Transport Administration and the police can cooperate in response to camera images and rapidly gain information about the extent of the crisis. Absence of a prearranged procedure for cooperation can delay information sharing, which may lead to the crisis becoming more serious.

Developing a predetermined cooperation procedure regarding the use of sensors and sensor data is an important step towards improved total defence capability. Cooperation regarding sensors

[1] The article is based on research performed in collaboration with the police.

can be crucial in ongoing crises or social disruptions, where current, accurate and continuously updated situation awareness is required to avert an event.

Currently, there is no formal cooperation plan involving sensors and sensor data. Rather, cooperation takes place on an ad hoc basis when emergencies arise. When cooperation does take place, it is often based on personal contacts between individual officials at the authorities. There is a great risk that important personal contacts are missing and that the system is vulnerable to staff changes. The consequences of such an ad hoc system is an inefficient use of society's assets, as well as a lack of time and resources to manage any legal or organisational issues that may arise. Efficient total defence capability requires established routines for the exchange of sensor data and a preparedness to share and receive sensor resources from other authorities. Cooperation and collaboration have to function in everyday life in order to function in the event of a crisis.

Government agencies have specific tasks during crisis management and heightened states of alert. They are responsible for the planning of their own crisis and security management. If they have little or no access to sensors, they become particularly dependent on cooperation between authorities in a crisis.

In order for cooperation regarding sensors to be successful, it is of key importance for government agencies, rescue services and the Armed Forces to provide one another with more knowledge about each other's sensors, how they are used and what type of information they can provide. It is also of great value to provide more knowledge about how situational awareness can be improved by using sensor data. For instance, various types of data processing services can facilitate analysis of large data sets or provide a clearer image of an area. Unmanned flying vehicles with mounted cameras, known as Unmanned Aerial Vehicles (UAVs) or Unmanned Aerial Systems (UASs), can be used to collect information about areas that would otherwise be impossible to reach or hazardous to operate in. It is also possible to obtain a quick overview from the air, which is often crucial in a crisis.

The effects of a serious societal crisis are often felt for a long time after the event and far from the location where it occurred – for instance, this was the case after the terrorist attack in Stockholm. Therefore, there is a desire for integrated cameras in railway stations and underground stations, as well as along roads, railways and underground tracks. These types of cameras provide information on how the flow of people and vehicles are affected during a crisis.

Working together on the procurement of new sensors is another form of cooperation that could be of interest to government agencies. A joint procurement process could benefit standardisation, which in turn could facilitate sensor operation and sensor data management. In addition, this might lead to more favourable purchasing agreements, as authorities could use each other's competencies for the specifications about what sensor requirement to require.

Legal challenges

Swedish crisis management is largely based on inter-authority cooperation and cooperation between actors on the local, regional and central levels, as well as between various sectors. The regulations that apply in everyday life also apply in a crisis. The administration of Swedish government agencies is based on authorities having defined tasks and being independent of the ministries and each other. According to various legal regulations, authorities are required to cooperate, but there are no indications as to how. Consequently, situations requiring cooperation could arise, where legal regulations that are applicable to the everyday operations of authorities could hamper effective cooperation.

Another aspect of inter-authority dependency is that authorities are generally bound by confidentiality. Confidentiality protects the information assets of an organisation and the individuals connected to its operations, and confidentiality is transferred to other authorities to a varying extent. The fact that one authority has access to a particular type of sensor or sensor data may constitute sensitive information from a security perspective, as it reveals the capabilities of the authority and thereby the country. Together, this means that confidentiality regulations limit the possibilities for authorities to cooperate.

The General Data Protection Regulation (GDPR), which protects individuals' privacy and personal information, could further complicate inter-authority cooperation. Sensors often register personal information, but according to GDPR, this is only allowed for specific purposes that are determined by the authority in charge of the camera. If personal information is shared, it will be used for a different purpose than originally intended, which may be prohibited. GDPR also forms the basis for the new camera surveillance act, which requires that most authorities apply for a permit to set up sensors.

In summary, inter-authority cooperation regarding sensors is legally complicated, but not impossible. It is therefore important that legal advisors take part in the early stages of the development of cooperation methods and technology, that is, in the planning

phase at each respective authority. At this early stage, technology and methods can still be adapted to ensure that cooperation takes place in a successful and legally correct manner. The planning for inter-authority cooperation regarding sensors should take place before the need arises.

Organisational challenges

Cooperation regarding sensors and sensor data is a complex task, and several perspectives need to be considered. These include technical compatibility, legislation, information security, and, not least, harmonising processes. Not all authorities need to work identically, but their interaction and performance of joint activities should be carried out in a manner similar to each other.

Cooperation regarding sensors fundamentally involves an exchange of technology, leaving little room for improvisation. Cooperation regarding technology also requires planning. However, preparing for cooperation regarding sensors is difficult, as no part of the government has overall responsibility. Nonetheless, all government agencies are required to support each other.

Communication and an understanding of each other's operations are prerequisites for cooperation between authorities. Consequently, a joint conceptual framework is required and joint activities need to be continuously performed. Descriptions of sensors and sensor data varies between authorities, which is natural, as their operations and purpose for using sensors differ. One example is what the police and other civil authorities refer to as surveillance systems. In the Armed Forces, these are known as intelligence systems. Another example is unmanned flying vehicles, such as UAS or UAV, also referred to as Remotely Piloted Aircraft Systems (RPAS), or drones in general. These designations are used both between and within authorities. Semantic differences can easily result in confusion and misunderstanding.

Knowing what support can be obtained and by whom is a central challenge. For various reasons, many authorities do not reveal information about their sensors or the performance of them. It is therefore not practical to compile information about them. However, through continuous dialogue and joint exercises between authorities, knowledge about each other's capabilities will gradually increase. Moreover, authorities will become increasingly confident in each other, which facilitates cooperation. Yet, there will probably always be surveillance resources that are too sensitive to share.

By designing common guidelines, the differences between authorities could be bridged and the risk of misunderstandings

reduced. These guidelines should include a classification (taxonomy) for various types of sensors and applicable standards, as well as an overall method of cooperation regarding sensors, describing the issues to be addressed and considered. Discussing types of sensors in principle is not as sensitive as discussing real, specific sensors, as performance or weaknesses do not need to be revealed.

Technical challenges

Sensors often generate large data sets. Analysing sensor data manually and identifying critical information in such large data sets is complicated. It is also difficult for a human operator to maintain concentration for the required period of time. Data processing services could therefore be used to support the operator by automatically distinguishing critical information.

Modern sensors are becoming more and more advanced, frequently demanding specially trained operators to manage them correctly and interpret sensor data. It is likely that this will become even more problematic as new and more advanced sensors are introduced. In the future, it will probably not be meaningful to supply the sensor alone, but specially trained staff will also be required. Cooperation regarding sensors thus entails sharing both technical and human resources.

The way forward

Successful cooperation regarding sensors will require a change in the work procedures of authorities. Inter-authority cooperation also requires cooperation between functions within and between the authorities, and on different levels within them. This applies to an exchange of information as well as development of new methods and tools for cooperation. Besides involving legal advisors in the early planning stages of the technical aspects of information sharing, there is also a close connection to the authorities' security functions.

Over time, rapid technological development will provide authorities with new capabilities and challenges, both in terms of technological systems and legally. This will raise questions such as how authorities should manage sensor data sets, how the sensor data should be used and by whom, who owns the information, and when and how it should be visualised.

For cooperation regarding sensors to be successful under pressure, it needs to be developed in an orderly fashion, prior to a potential crisis. Authorities that could reasonably be expected to send and receive sensor data need opportunities to practise. All the

cooperation steps to be taken in a crisis must also function in everyday life.

In order to progress, it is necessary for authorities to prioritise the development of cooperation and engage in activities to strengthen crisis management organised by the Swedish Civil Contingencies Agency (Myndigheten för Samhällsskydd och Beredskap, MSB). It is also necessary for authorities to develop a climate of cooperation, where exchange of sensor data and connected resources is regarded as natural and as enriching each party's area of responsibility. To achieve this, it is important that operative units receive sufficient support so that they can immediately start developing ways to cooperate regarding sensors. As a result, in the event of a crisis, established routines would already be in place. If this could be ensured in Sweden, total defence capabilities and crisis management would be considerably strengthened – without major investments.

7. Long-term challenges for Sweden's materiel supply

Per Olsson

Sweden's materiel supply is facing major challenges. The Swedish Armed Forces is facing a deteriorating security situation in our immediate neighbourhood, while at the same time much of its existing military equipment will reach the end of its service life and need to be replaced. Today, there is broad political agreement on the need to increase defence spending in order to strengthen Sweden's military capability, but cutbacks after the Cold War have created considerable equipment needs. Increased costs for increasingly advanced equipment will place extensive demands on efficiency and on prioritising in procurement and utilisation, for both the government and Parliament, as well as for the Swedish Armed Forces. This is in order to maximise the potential capability from the investments that are now being made.

A deteriorating security situation after historical cutbacks

Sweden's biggest security policy challenge is Russia's increased military capability and the Russian leadership's increased readiness to use this capability to achieve its political objectives. At the same time, historically stagnating and reduced defence budgets in Western Europe, after the end of the Cold War, have meant that a Western technological advantage over Russia can no longer be taken for granted.

The problems caused by the historical cutbacks in Western European defence budgets have not only had consequences for security policy, but also for the defence industry. From this perspective, even friendly states are competitors. Amongst other things, relatively small defence efforts in Europe have meant that the US has been able to consolidate its technological advantage in an increasing number of areas in the defence equipment market. At the same time, new defence industrial actors have begun to take shares of the international market. For example, South Korea has recently sold artillery, in the form of self-propelled howitzers, to Norway, Finland and Estonia. At the same time, more of Western Europe's traditional export customers, such as India and the Gulf States, are investing heavily in building their own defence industrial capabilities.

Russia's illegal annexation of Crimea in 2014 and ongoing military intervention in eastern Ukraine are major contributing factors in

recent years to several Western European countries beginning to increase their defence expenditure, including equipment appropriations. For European NATO members, pressure from the Trump administration is also an important factor, and several pledges have been made to meet the Alliance's objective of spending at least two per cent of GDP on defence. In Sweden as well, defence spending has increased, and there seems to be broad political support for further investments. In recent years, Sweden has decided on or implemented a number of significant arms acquisitions. The Swedish Armed Forces has, amongst other things, been supplied with self-propelled artillery pieces called Archer, and a decision has been made to acquire the latest variant, version E, of the JAS 39 Gripen fighter aircraft submarines of a new class, A26, and the American Patriot air defence system. In addition, decisions have already been taken that a large number of tanks and combat vehicles will be renovated and that submarines from the Gotland class will be upgraded.

New needs for equipment

Efforts to strengthen the country's defence capabilities are complicated by the fact that the Swedish Armed Forces acquired several of its current systems during the 1990s, and that these will need to be replaced or upgraded within the next ten to 20 years. The early 2000s saw the acquisition of equipment focused on international operations, but the deteriorating security situation in Sweden's immediate neighbourhood has prompted a renewed focus on national defence. This has led to an extensive need for renewed capabilities, such as a stronger air defence as well as modernised control systems and improved logistics. Rapid technological development has also created completely new needs for investments, such as in cyber capabilities. If these systems and capabilities are not replaced or introduced, Sweden's combined military capability in relation to the outside world will decrease rather than increase. These challenges are not uniquely Swedish, but pose problems for most Western European countries. However, this is hardly a consolation, as European countries rely on each other for their security, either through bilateral agreements, within NATO, through partnerships with NATO or through membership of the EU.

Despite the efforts now being made, equipment needs over the next ten to twenty years will be extensive. The Swedish 'Equipment Demand Inquiry' (*Materielbehovsutredningen*) found that up to 168 billion Swedish kronor may need to be injected between 2021 and 2030 if the operational capability of the military units is to be increased in order to address the deteriorating international situation. This includes raising the so-called 'foundation', i.e. bare

necessities such as uniforms and spare parts. It includes upgrading the navy's corvettes, but also an improvement of control systems and protection of bases. The inquiry proposes only modest increases in volumes of units, whereas the Swedish Armed Forces, in its long-term study, the *Perspective* study. from 2018, proposes significantly increased volumes of the number of weapons systems and units. If the Perspective study's ambitions were to be realised, this would mean an almost doubled defence budget compared to today.

High requirements create increased costs

However, the doubling of expenditure does not automatically mean a doubling of the armed forces. This is because the cost of defence equipment has a habit of increasing exponentially over time. For example, the cost of each individual fighter aircraft has historically increased by an average of seven per cent annually, corresponding to a doubling of costs every ten years. The corresponding figure for submarines is four per cent, and seven per cent for naval vessels. This development is a consequence of military equipment becoming increasingly advanced. In addition to growing demands for increased firepower, level of protection and mobility, modern weapons systems also require increasingly sophisticated sensors, such as radar, as well as robust networks for an increased capability to fight alongside other parts of the armed forces.

The incentives to keep up with technological developments are strong. Countries that lag behind are at risk of fighting the war of the future with obsolete equipment. On the other hand, there is a risk that too much focus on high quality items will force countries to reduce the number of weapons systems and units, which is what has happened in Sweden. The trend is not uniquely Swedish, however. In recent decades, several Western European countries have chosen to change from quantity to quality. The consequence has been that small countries such as Sweden, Norway and Denmark can now count several types of units in a few or single figures.

Need for efficiency

There have been numerous attempts to curb the increasing costs of military equipment. For example, in several Western countries during the 1990s, the recommendation was to purchase equipment already on the market or 'off-the-shelf'. The reason was that existing systems could be introduced more quickly and cheaply than if new equipment was to be developed domestically. International collaborations on equipment were also sought, as it was assumed that these could lead to economies of scale where

development costs and other fixed costs would be distributed between a larger number of production units.

Sweden's current principles for equipment supply are formulated based on the insights above, with the aim of counteracting cost increases and reducing the time it takes for weapons systems can be put into service. The government's current principles for equipment supply from 2009, as well as in the Materiel Supply Strategy (Materielförsörjningsstrategin) from 2007 of the Swedish Armed Forces and the Swedish Defence Materiel Administration, state that cost-effectiveness and fast delivery should be prioritised. In the first instance, the existing equipment systems of the Swedish Armed Forces should be maintained. Subsequently, the procurement of equipment already on the market should take place. Only in the final instance should new equipment be developed. In all cases, international collaborations should be considered in order to achieve economies of scale. However, the operational capabilities of military units take precedence over all other priorities. After all, cost effectiveness is not the same as low cost, but is rather a question of the greatest possible result for the expense.

Maintaining certain equipment systems for longer periods of time is one way of maintaining larger volumes of units at a relatively low cost. A nearby example is the Finnish army, which sometimes acquires used equipment and also retains older equipment for longer compared to other Nordic countries. For Sweden, this approach could remedy the decreasing volumes of units, but might also lead to less desirable consequences. Some units would need to settle for obsolete equipment, which would limit how they can be used operationally. In addition, old equipment can cause problems from a supply perspective since spare parts for older systems often cease to be manufactured after a number of decades.

So how does it look for Sweden? The economically large equipment systems acquired and planned in recent times give a clear indication that most of these systems are newly developed. The Archer artillery system and JAS 39 Gripen E fighter aircraft, Helicopter 14 and submarines of the A26 class are some examples. Acquisitions of existing equipment on the market are relatively few; however, Helicopter 16 and Armoured Modular Vehicle 360 are usually mentioned as examples. It is easy to conclude that the Government's principles for equipment supply have not been complied with, but then it is not known how much existing equipment would have been acquired without the principles. In addition, the operational capabilities of the Armed Forces take precedence over all other priorities. This criterion is extremely

difficult to assess and may well justify a high percentage of newly developed systems.

In addition, the government and parliament themselves have made considerable deviations from the principles for equipment supply through the designation of three essential security interests. Today, these comprise fighter aircraft capability, underwater capability and the so-called integrity-critical parts of the command and control system area. By highlighting essential security interests, a targeted procurement of fighter aircraft, submarines and command and control systems is made possible, which underlines the continued close relationship between Sweden's Armed Forces and defence industry.

In other words, there is no indication that the acquisition of advanced and newly developed equipment has decreased or will decrease in the near future. There is therefore a risk that the trend of increased equipment costs will continue in the future.

A need for priorities

However, the question of advanced but expensive versus more but cheaper equipment is only one of the trade-offs that political and military decision makers have to address. For the government and parliament, the first step is the resource issue, where the needs of the Armed Forces are set against other resource needs in society. This also applies to the other parts of the total defence.

Most indications are that defence will receive increased resources in future, but additions must be both adequate and be made available at a rate so that the Swedish Armed Forces can absorb the increase. The Swedish Armed Forces must in turn define a clear order of priority regarding which measures need to be taken first. Either way, investments in equipment need to be made with military staffing, as well as the other strategies and doctrines of the Swedish Armed Forces, in mind. How well does the equipment supply strategy comply with other military strategic policies? How do we ensure that the equipment supply works together with the reintroduced but limited conscription? These are just a few examples of questions of priority that decision makers face today and in the future.

Long-term planning for the supply of equipment should also include a strategy for the essential security interests. Today, there is no such clear strategy, and also no clear and uniform definition of what these interests are. Under EU law, each Member State has the right to exempt defence equipment that meets essential national security interests from the Union's standard competition rules. But the fact that Sweden has identified whole ranges of capabilities, such as fighter aircraft capability and underwater capability, as

essential security interests, creates a need for clear definitions of what these capabilities include. The national security strategy of 2017 emphasises that essential security interests and associated industrial and technical competence should be maintained and developed, if it is militarily and financially rational. But what consequences does this have for the state's relationship with the industry, and what obligations, if any, has the state undertaken? These are questions that need to be addressed in the future.

There are many views in the debate about the benefits and costs associated with an extensive Swedish defence industry, but regardless of the position taken on this issue, long-term investments are required if the country's defence industry is to effectively contribute to the country's defence capability in the future. It is not just about investments in the acquisition and maintenance of equipment to keep the industry running, but also about investments in research and development that will facilitate the emergence of new concepts and cutting-edge technology in order to meet the needs and challenges of the future.

8. Who delivers if war breaks out? – On the business sector, security of supply and the future total defence

Jenny Ingemarsdotter and Jenny Lundén

The involvement of the business sector is key to the development of a comprehensive defence, including a robust security of supply system, i.e. planning for availability and distribution of food, medicine, fuel and suchlike. This was previously the primary function of what was known as the economic defence, a key element of the old total defence. The aim then was to provide for the population for a number of years in the event of the country being blockaded. Now, in the context of a reinstated total defence planning, goals and objectives for a national security of supply are discussed once again. Involving the business sector at an early stage in the development of such a security of supply system is essential. But which requirements and conditions have to be considered in this context today?

The business sector and security of supply

The objectives and level of ambition for the redevelopment of a national security of supply are ultimately a political matter, largely involving offsetting costs against risks. In contrast to the crisis management system, which focuses on relatively short-term crises, discussions are now focusing on the risks of prolonged disruptions, grey zone situations between peace and war, and – ultimately – armed attack. These scenarios bring to the fore the need for a national security of supply.

The business sector plays a significant part in building a robust total defence as vital societal functions such as telecommunications and power supply, previously state-owned, are now in many cases operated by private corporations. This situation has resulted in many analyses and committee directives in the context of Sweden's renewed total defence planning. In short, the role of the business sector in the future total defence has become a hot topic – but what is actually being said?

One fundamental challenge has to do with implementation – how the business sector can participate in practice in the development of the total defence. This may involve identifying and regulating enterprises important for the war effort, so-called 'preparedness contracts' with companies in the business sector, and possibly a central business council. Addressing some of the most common

issues and proposals regarding the future role of the business sector in the total defence, this chapter focuses specifically on the challenges involved in building a robust security of supply. It also highlights the business sector's own perspectives and interest in the development of a new total defence concept.

A HISTORICAL BACKGROUND

Terms and concepts such as 'K-företag' ('enterprises important for the war effort'), preparedness planning and security of supply planning date back to the total defence that existed in Sweden throughout the Cold War. It is important to include these historical experiences when developing a new total defence concept for our present-day society: they can help us understand both the differences and the similarities between the conditions that existed then and those that exist now.

Bearing in mind experiences from the First World War, when Sweden suffered from food shortages and trade disruptions, the governments after the war drew the conclusion that the entire economy – including the business sector – had to get involved to guarantee access to strategically important products such as fuel and food in case of a future conflict. The National Swedish Commission of Economic Defence (Rikskommissionen för ekonomisk försvarsberedskap) was established in 1928 with a view to structuring these efforts. The development of a national security of supply system continued over the decades that followed. During the Second World War, it was concluded that modern warfare would affect the civilian population and the whole of society. This required a "total defence" that would build up the endurance and mental preparedness of the population. The economic defence system would continue to play a key part in this total defence.

From the 1960s onwards, the National Swedish Board of Economic Defence (Överstyrelsen för ekonomiskt försvar, ÖEF) took responsibility for the government's strategic stockpiling of goods that were not produced in Sweden and could be used to supplement the business sector's own stocks. ÖEF coordinated detailed planning to meet companies' needs in wartime of labour, raw material, energy and transport. Collaboration between the business sector and the government also took place via the National Board of Trade, working on methods to enable foreign trade to continue operating in times of crisis or war.

As part of the economic defence system, the government established contracts with selected companies. These 'enterprises important for the war effort', as they were known, would continue operating in times of crisis or war, sometimes with a realigned production focus. There were a number of advantages for the

companies selected: their personnel was relieved from other duties within the total defence, they were given priority access to the repair of telecommunications and they were exempted from fuel and transport rationing. These selected companies had a number of tasks to perform: producing substitute goods or stockpiling strategic raw materials, for instance. Such measures came about due to concerns during the Cold War that blockades, would be imposed, and that Sweden in such a situation would risk being cut off from the outside world.

Preparedness planning and the system with 'enterprises important for the war effort' were phased out towards the end of the 1990s. The end of the Cold War meant that it was no longer considered necessary to maintain such an ambitious security of supply system, a relatively expensive undertaking. More specifically, the strategic stockpiles were now sold off or liquidated and the so-called preparedness contracts with companies in the business sector were terminated.

The carrot and the stick

When the old total defence system was phased out, one thing was left intact – the legislation regulating the powers of the government. The government still has the right to control the resources of private companies in certain circumstances: for example, property, industrial plants, ships and vehicles can be utilised on behalf of the government during a heightened state of alert and war. This legislation was developed in a historical context when it was assumed that resources were available within Sweden's borders and that companies had stocks of their own. There is a major contrast between the situation then and present conditions, with just-in-time deliveries and minimal stockholdings. In a world of globalised supply chains, governments cannot expect resources to be available when they are needed the most – unless plans have been implemented to deal with such situations.

Efforts to strengthen Sweden's security of supply may be based on existing legislation and regulatory frameworks, but adaptation to present circumstances may be necessary. For example, as the Swedish Defence Commission proposed in its report Resilience (Motståndskraft), demands could be made of companies to stock certain strategically vital products. Other types of requirements could involve improving the resilience and protection of vital societal functions, including information security. Of course, companies have a vested interest in developing their abilities to withstand incidents such as disruptions and intrusions in order to maintain production and operations. From a total defence perspective, however, a joint approach is also needed in which private and public stakeholders join forces, working on the basis of

a shared level of ambition and a shared understanding of threats as well as shared considerations of what needs to be protected.

Access to relevant contacts and networks is a "carrot" that could be used to get the business sector involved in this work. By comparison, Finland has been running exercises and total defence courses of various kinds with the business sector for a long time, and this is thought to create valuable networks within and among different sectors and industries. Finnish companies providing vital societal functions base their emergency response measures on commercial interests in contracts and by means of risk management. Finnish preparedness measures, both in the business sector and in society in general, are coordinated via the country's National Emergency Supply Agency.

Regardless of how the business sector is involved, a collective understanding in the public and private sectors of what needs to be done will be key to the ongoing development of a new total defence. However, the effect of enhanced collaboration between the public and private sectors will be limited unless economic resources are added. Although the business sector may be interested in participating in the development of the total defence, individual companies cannot be expected to bear major costs that are not commercially motivated. This is why the Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap, MSB) and the Swedish Defence Commission have indicated that there is a need to develop a comprehensive financing model.

Security of supply 2.0

Given the societal changes that have taken place since total defence planning was phased out in the late 1990s, it is necessary to consider a number of issues prior to redeveloping the security of supply. For example:

- Which goods and services should be regarded as strategic or vital to society?
- Is stockpiling the way forward? And if so, how should turnover and distribution roles – for instance – be divided between private and public stakeholders?
- To what extent should methods other than stockpiling be considered, such as production reorganisation, preparedness contracts or a new type of contract?

Although the answers to these questions will differ depending on the sector, it is clear that business sector stakeholders will play an important part in making decisions in different areas. In 2017, the Swedish Defence Commission proposed that a business council

should be established. This should complement existing trade association fora and aim for a mutual exchange of information. A business council would jointly develop approaches, plans and terms for collaboration between public and private stakeholders.

The Swedish Defence Commission also proposed the reinstatement of some kind of 'enterprises important for the war effort'. Regardless of which configurations may be of relevance in this regard, trends such as streamlining, globalisation and digitalisation have significantly changed the playing field in the business sector compared with the time of the previous total defence. Besides goods, a large number of services must now also be regarded as strategic. These include digital systems enabling distribution of medicinal products and foods, but also personnel who are able to manage these systems. Identifying which stakeholders, goods and services are to be defined as strategic in the society of today is an important challenge. Even if 'enterprises important for the war effort' were reintroduced, this would not be the only model for the business sector's involvement in the total defence. Preparedness perspectives can reasonably also be dealt with more generally in various contracts and procurement procedures.

Business representatives are generally positive to the Swedish Defence Commission's proposals as long as the terms and conditions will be reasonable, such as taking into account competition neutrality and models for financing. Many companies also consider it important that roles and responsibilities are made clear and that the total defence planning is carried out with a long-term perspective.

Three success factors

Concepts such as 'enterprises important for the war effort' and business councils are, in a way, simple and concrete factors that can be used in debates on the role of the business sector in the total defence of the future. At the same time, it is important to establish certain basic criteria before focusing on forms of collaboration. These can be summarised in terms of objectives, responsibilities and communication.

As regards objectives, the business sector and the authorities have long demanded greater clarity in terms of the ambition level of the total defence. Such ambitions may range from providing the general public with the "bare necessities", to securing round-the-clock Internet access. Without any objectives at all, it is difficult for individual authorities, municipalities and county councils to specify reasonable preparedness requirements within the framework of public procurement procedures, for instance.

Companies have also requested clarifications regarding the distribution of responsibilities between various public stakeholders in the context of security of supply issues. The issue of greater clarity in terms of who "owns" situations within and among different sectors – energy, food, transport, etc. – is often brought up.

Finally, communicating the objectives, ambitions and tasks of the total defence to relevant stakeholders is important. Regardless of specific forms of governance and methods, a collective understanding in the public and private sectors of the threats faced and what needs to be done will be a key factor for the success of the ongoing development of a new total defence.

9. Synthetic biology – opportunities and challenges for the total defence

Fredrik Ekström, Jonas Näslund and Per Stenberg

Imagine a total defence where plants change colour to warn against toxic gases, where civilian and military emergency service vehicles are powered by fuels produced from micro-organisms, where crops are designed to cope with a changing climate. With protective substances circulating in the body, chemical warfare agents are broken down before they have time to cause injury. These concepts are not science fiction but have already been demonstrated in laboratories. The development in synthetic biology is rapid and has the potential to have a revolutionary impact on the capabilities of the total defence. But the development also leads to new risks because the enemy can use synthetic biology for its own purposes, for attacks against agriculture, genetic assassinations, and more.

The significance of synthetic biology for the total defence

Development and applications in synthetic biology already affect important parts of civil society, and the potential for the total defence of the future is considerable. The production of important medicinal products, as well as advanced antidotes against chemical warfare agents, is already a reality. Crops designed with an inherent climate and pathogen resistance, i.e. resistance to harmful viruses and bacteria, amongst other things, can contribute to Sweden's food security and forestry in the event of a warmer climate. Organisms can be designed to indicate the release of toxic substances, to purify drinking water, and to clean soil from toxins and environmental pollutants. Genetically modified algae and cyanobacteria are already used for small-scale production of biodiesel and other fuels from locally available raw materials, such as forestry residues. In the longer term, the development will provide new materials with completely new properties. A more speculative outcome in the long term is that development may include genetically modified soldiers that withstand chemical and biological warfare agents or with improved physical strength and endurance.

An intrinsic problem with development is that the same technologies used to do good can also be used for illicit purposes. Despite the opportunities for abuse being to some extent limited by international regimes through legislation and control bodies,

the methods and knowledge for modifying or moving genes between species, for example, are universal, regardless of the properties added. Designed, highly contagious, micro-organisms that evade both detection and medical treatment are an obvious threat. A hostile attack with a designed micro-organism is likely to require a rapid response, such as in the form of an advanced antidote. There is a legitimate concern about genetic assassinations and targeted genetic weapons designed to knock out specific parts of the genome. However, it is important to note that antagonistic applications of synthetic biology do not necessarily have to be directed against the Swedish population, even agriculture and forestry are potential targets for an attack. A high level of knowledge is required by the Swedish authorities affected to understand the nature of the threat, but also an infrastructure, including laboratories and specialist expertise, designed to quickly use the knowledge of the threat and implement effective countermeasures.

Examples of the current use of synthetic biology

It is likely that synthetic biology will have a profound effect throughout most of our society. The applications are found in many areas, making it difficult to provide a comprehensive picture. To illustrate the potential, some of the areas where synthetic biology has already made big impressions are described below.

Provision of medicinal products. Enzymes are substances of biological origin that increase the rate of chemical reactions; they are involved in almost all of the processes that occur in living organisms and are therefore a prerequisite for all life. Enzymes convert sugar into energy, allowing plants to absorb carbon dioxide from the atmosphere and giving bacteria resistance to antibiotics. Transferring the gene that encodes an enzyme between different organisms is nowadays routine practice. As early as a decade ago, genetic material was transferred from summer wormwood to baker's yeast. The new genome gave the yeast cells the ability to produce a substance that can be easily modified to Artemisin, a medicinal product recommended by the World Health Organisation (WHO) for the treatment of malaria. More recently, chemical processes have similarly been created by combining genetic material from widely different organisms. One striking example is yeast cells modified with over 20 genes from mammals, plants and bacteria to produce opioids, which are medicinal products used for analgesic treatment and palliative care.

An excellent illustration of the possibilities of synthetic biology for the total defence is the development of enzymes capable of breaking down chemical warfare agents. The development of

these enzymes has largely been realised by directed evolution in a laboratory environment. The modified enzyme breaks down some nerve agents more than 17,000 times faster than the natural enzyme, and experiments show that animals treated with the modified enzyme have significantly improved tolerance to nerve agents. Directed evolution today is a technique widely used in various applications, something that was acknowledged by the 2018 Nobel Prize in Chemistry.

Living sensors. Sensors that detect chemicals are important in many contexts, ranging from detecting emissions from industries to preventing import of illicit substances. Using plants as living sensors is an attractive proposition because they can live in a variety of environments if they are provided with sunlight and water. A research team recently managed to utilise the thale cress plant to create a highly sensitive biosensor for the detection of fentanyl. Fentanyl is a very potent analgesic that is also produced illegally and has caused several deaths among drug users.

The detection of fentanyl is complicated since the molecule exists in many different three-dimensional structures. With the help of computer modelling, the researchers first designed a number of proteins that should theoretically bind to the most common forms of fentanyl. This can be compared to designing locks to fit specific keys. The genes of these proteins were synthesised and then introduced into plants, along with a signalling system that made the plant luminous when in contact with fentanyl, in the form of a solution. There are many other projects underway that attempt to utilise plants and other organisms as sensors for the detection of everything from emissions of chemicals into the environment to early detection of human diseases. One example of the latter is a project where researchers are trying to create bacteria that can detect cancer, or infections of the gut. If necessary, the bacteria could potentially release pharmaceuticals that they carry themselves.

Food security. The supply of food to the population during a protracted crisis could be a significant challenge, especially if Sweden is simultaneously exposed to adverse operations targeting agriculture, or if import trading routes have been affected. Perhaps the most obvious use of synthetic biology is to modify existing crops so that they have improved resistance to plant pests or can be cultivated despite changing climates. It is also possible to modify crops to improve nutritional value or productivity. There is ongoing development to use cells as factories to produce special nutrients or completely new foodstuffs. In the long term, perhaps it will be possible to develop micro-organisms that

produce foodstuffs that have their natural origin in the plant or animal kingdom.

Human modification. With today's technology, it is not only possible to change specific parts of the genome, but also to remove or add whole genes. For example, there are medicinal products used to treat different types of blood cancer that are based on the patient's own immune cells being genetically modified so that they target and kill the cancer cells. The modification takes place using a virus that delivers new genetic material to the immune cells.

Investments in synthetic biology

Globally, a considerable amount of money is being invested into synthetic biology and the development could lead to a new industrial revolution. Influential nations such as the United Kingdom and the United States are also investing a significant proportion of their defence research budgets into synthetic biology. One concrete example is the US Defence Advanced Projects Agency (DARPA), which increased its investment into synthetic biology by $100 million between 2010 and 2014. Sweden is a nation that is investing a significant proportion of its GDP on research. However, compared with other countries, it does not invest as much into biotechnology, the field in which synthetic biology lies.

In Sweden there are no investments being made to exploit synthetic biology and utilise its potential in order to increase the Swedish total defence capability. The consequences are potentially serious, and also limit Sweden's readiness to face antagonistic use of synthetic biology. Global differences are not just found within funding; legislation also varies considerably. For example, China has more permissive legislation in this area, which, amongst other things, enabled genetic modifications of human embryos. The United States also has far more permissive legislation than the EU.

The way forward

Today, synthetic biology largely focuses on modifying biological systems which already exists in nature. For example, an existing enzyme can be modified to withstand a higher temperature, which is required in many industrial processes. Designing a new enzyme with completely new properties is much more difficult. To do so, very many so-called 'design-build-test' cycles are often required, which becomes very resource intensive. In order for synthetic biology to mature and fulfil its full potential, increased knowledge of complex biological and chemical systems is required. Academic research is therefore important for the future development of

synthetic biology. In addition, authorities and other actors, such as the biotech industry, must increase their expertise in synthetic biology in order for Sweden to be able to take advantage of the opportunities in this field. Another fundamental prerequisite for fulfilling the potential from a total defence perspective is effective interaction between academia and the total defence authorities. The step from a basic understanding of synthetic biology to a use that is relevant to the total defence is significant. One challenge, for example, is to adapt concepts that work on a laboratory scale into industrial production, which requires a close collaboration with industrial partners.

What should be prioritised today is research that links the progress in basic research with the needs of the total defence. In defence-related research, the focus should be on developing methods, knowledge and infrastructure in synthetic biology. Only when these conditions are in place can products and solutions directly aimed at Sweden's total defence needs be developed. Well-balanced investments with clear objectives provide opportunities to tailor the research to Swedish needs, and make Sweden an attractive partner in the international arena.

10. Cyber defence – skill needs practice

Tommy Gustafsson and David Lindahl

Since the turn of the millennium, cyber incidents and suspected cyber operations have had a profound impact on many countries and organisations. Sweden has a high degree of digitalisation of vital societal functions and the individuals who handle these systems daily play a key role in our total defence.[2] It is therefore important to hold regular exercises for these people in how to handle cyber incidents. Currently, too few exercises are taking place, and it is also difficult to implement them realistically and pedagogically. Ensuring the national total defence capability requires relevant training environments, increased exercise volume, and research into training methodology.

Cyber operations

Cyberspace is an arena where both operational capabilities and doctrines have evolved significantly over the recent decades. It is an arena where the interests of military and civilian actors meet, and the threat from cyberattacks poses new challenges for Sweden's total defence. A conventional conflict is limited by geography; for an enemy to be able to strike against Sweden, it must first pass the border, through the protection provided by the Swedish Armed Forces. A cyber operation, i.e. activities in cyberspace perpetrated by a state to achieve military or political objectives, allows an attacker to strike against all the computers that are accessible for communication without the conventional defence forces being able to do anything about it.

As a consequence system administrators in civilian organisations risk being thrust into the front line of the conflict, in which case they will need the skills not only to ensure that systems are resilient enough but also skills to handle attacks.

Today, cyber operations are used on a regular basis for intelligence gathering, industrial espionage and sabotage. International conflicts have occurred wholly or partly in cyberspace. There are examples of cyber operations where nations have attacked civilian targets, both directly and indirectly, using proxy organisations such as hacker groups. During the war between Russia and Georgia in 2008, more than one-third of Georgia's internet was seriously disrupted, governmental communications were stopped,

[2] The total defence is the Swedish term for the civil defence organisations and the armed forces combined.

and the National Bank of Georgia was forced to shut down all computer services for 11 days.

The cyber arena is also used for various types of influence operations. Most influence operations seem to be focused on manipulating public opinion on a particular issue. However, there are cyber operations that may have been used to influence the strategic decisions of sovereign nations. One such example is the 2009 cyberattack against Kyrgyzstan while it was negotiating to host a NATO base on its territory.

It is difficult to limit the effects of cyber weapons, such as malicious code, and cyberattacks. In 2010, the Stuxnet cyber weapon went well beyond its intended targets in Iran, and seven years later the NotPetya attack not only disabled ten percent of Ukrainian computers, but also spread beyond the country's borders and became the world's most costly cyberattack to date. Overall, developments within the cyber arena show that a threat to Sweden's vital societal functions exists, even when Sweden is not the intended target of a particular attack.

Cyber defence capability needs

Many cyber security frameworks and guidelines highlight the need for knowledge about threats and protective measures. Amongst other things, this knowledge is necessary to utilize the available resources in the right way, for instance by prioritising technical and administrative protective measures. Proactive measures are important and it is often the knowledge and actions of individual system administrators that determine if an incident occurs and whether or not its consequences become serious. A good way to create this knowledge is to participate in exercises. Exercises provide experience-based learning without having to deal with actual incidents. Through practice, system administrators become more skilled and the systems more secure.

Cyber exercises such as the Locked Shields and Crossed Swords exercises arranged in Estonia, and Cyber Czech in the Czech Republic, are used internationally to increase defence capabilities,. Arranging exercises is also in line with Sweden's national cyber security strategy from 2017, which amongst other things, states that 'Regular national and international training is a prerequisite for developing and evaluating structures to manage serious IT incidents...'.

In addition to the level of knowledge of individual system administrators, collaboration has been shown to be a key factor for quickly and effectively managing advanced large-scale cyber incidents. When Estonia was attacked in 2007, it benefited greatly from a national collaboration established between system

administrators from different organisations providing vital societal functions. Exercises are a way of establishing a foundation for this type of collaboration.

Enhancing the national capability

To enhance the Swedish national capability in the cyber area, there are three major challenges that need to be addressed: firstly, access to relevant training environments and scenarios; secondly, an increased number of exercises; and thirdly, research is needed to ensure that the right skills are properly taught.

In order to create relevant training environments and scenarios, considerable knowledge is needed not only of IT, but also of current cyberattacks. Furthermore, a pedagogical proficiency to develop exercises that convey the complexities involved in cyber incidents is needed. Ideally, exercises should be conducted in operational IT environments, but this is rarely possible since it might cause disruption in the very systems the participants strive to protect.

An alternative is to create a replica of the IT environment in question, but most organisations lack sufficient resources to prioritise setting up parallel IT environments. Even if the technical systems were copied, it would be very difficult to simulate the activities of the users, thus limiting the relevance of the scenarios. A 'quiet' network, where only the attackers and trainees are active, differs greatly from reality.

Another problem is that there is often a need for several iterations of an exercise before the pedagogical elements work optimally, and the rapid changes in the IT field means that exercise environments quickly become obsolete. Most organisations are too small to continuously develop training environments and scenarios.

There are some commercial initiatives available, but these have so far lacked relevant training environments for the total defence. Resources for developing in-house exercises must therefore still be set aside by the organisation that is planning to arrange them, which exacerbates the difficulties described above. In cases where the commercial initiatives are foreign-based, this entails a security problem from a total defence perspective. Overall, the difficulties involved in developing and maintaining training environments and scenarios, as well as the lack of relevant commercial alternatives, mean that an investment in the total defence in this field is needed.

Similar initiatives are already taking place in several countries, with prominent examples in Estonia and Norway. These aim to strengthen the national cyber defence capability in each country

and often include actors from the armed forces, civil authorities, actors in the vital societal functions and higher education institutions. This mix of participants ensures that the exercises are based on relevant technologies, real-life scenarios, and are sufficiently widespread to have a positive and long-lasting impact on national cyber defence capabilities. A key component of these initiatives is the establishment of a national cyber range, where exercises can be developed and implemented.

In collaboration with the Swedish Civil Contingencies Agency and the Swedish Armed Forces, FOI operates the Cyber Range And Training Environment (CRATE) facility, which is used in research projects as well as in exercise and course activities. It has now become an advanced cyber range and includes a comprehensive IT infrastructure, as well as a number of specially developed tools for developing and holding exercises. CRATE could provide a good basis for a Swedish national cyber range.

The challenge to increase exercise volume requires both greater awareness and better access to relevant cyber security exercises. Many organisations that carry out vital societal functions are unaware of their role in Sweden's total defence capability and therefore of the importance of their cyber security capability. They primarily design their security activities to manage operational disruptions and would probably not prioritise cyber security exercises, even if such exercises were available. Improving exercise opportunities alone without raising awareness would therefore not lead to increased exercise volume.

To address the challenge of ensuring that the right skills are properly taught, educational research in relation to cyber security is required. Even though Sweden, like many other countries, has conducted exercise and training activities for more than a decade, there has only been limited research in this field. Arranging exercises with a focus on the needs of the total defence appears to be a workable method, not least considering the effects this will have on future collaboration, but further research is required to substantiate this.

Other important research issues in the field include technology and method development in cyber ranges, methods for increasing the exercise volume as well as how exercises can be used to generate decision data for future research. International examples also show that a national cyber range can be used to contribute to skills provision in the longer term by allowing higher education institutions to utilise it in research and education.

By addressing the challenges of providing exercise environments, creating an increased exercise volume, and a knowledge expansion on these through research, Sweden's cyber defence capability, and thereby the total defence capability, can be enhanced to meet the challenges of the future.

11. Antagonistic electromagnetic threats to civil defence systems

Sten E. Nyholm, Tomas Hurtig, Kia Wiklundh and Sara Linder

Many of today's vital societal functions rely on electronic control systems and wireless communication systems, such as GPS, mobile phones, and Wi-Fi. Cyberattacks with malicious code have become frequent, but since wireless communication systems and unprotected electronics can also be sensitive to electromagnetic (EM) threats, such as jammers and microwave weapons, intentional EM interference constitutes a tangible threat to civil defence capabilities and their potential to support military defence. It is therefore important that EM threats are considered in the risk and vulnerability analyses that authorities, municipalities, county councils, regions, and private enterprises with operations within civil defence are obliged to perform on their undertakings, especially concerning operative capability during a heightened state of alert.

A plausible EM-threat scenario

Imagine the following: the last few months have been characterised by an increasing international split and an escalating number of confrontations between military vessels and aircraft in the Baltic Sea area. Many servers at central government institutions, news agencies and private companies are at risk of advanced cyberattacks and false information is spread daily in social media. The Swedish government considers a mobilisation of the total defence to cope with the situation.

At this time, a large number of societal systems experience EM interference and some cease to work entirely. The communications centres of the emergency services lose contact with field units. Passage and alarm systems at several power plants and government buildings are inoperative. Power grid disruption forces the engagement of emergency power facilities at hospitals and alarm centres. There is traffic chaos in the major cities when traffic lights stop working. Trains remain immobile on railway lines when signals and electric power are lost. Landline telephones and mobile phones only function intermittently. Water distribution fails since pumps do not have electric power. Citizens cannot buy food or refuel their cars since electronic payment systems are not working. The public is unable to receive radio or TV broadcasts to find out what has happened or what to do. Transportation of food, fuel, etc. is so difficult that food shortages arise and private vehicles are immobilised.

What has happened? It soon turns out that there are a large number of jammers placed in cars, bags, baby strollers, etc. in the proximity of communication centres, government buildings, and switching stations for electricity and telecommunications. Jamming equipment on unmanned aerial vehicles circulating over the larger cities and airports paralyse all wireless communication. Furthermore, electronic components inside vital devices have somehow been burnt in radio and TV transmitters, in control equipment of switchgear stations, and in government offices.

How is an EM attack mounted?

An electromagnetic attack is mounted using equipment that emits EM radiation at radio frequencies, which in its simplest form can be a common radio transmitter, mobile phone, etc. The attack can occur with narrow band radiation on only one or a few frequencies, or with broadband radiation covering all frequencies within a wide frequency interval.

A simple method is to use jammers transmitting inaudible radio frequency noise. This drowns out computer communication signals in the noise, and wireless communication in one or several frequencies is inhibited or impaired. The more powerful radiation from microwave weapons can disrupt the operation of electronic components, such as transistors or microprocessors, making them either temporarily malfunction or lose their function altogether, or actually frying components via currents induced in the circuits by the EM-radiation. The difference between these modes of attack is that jammers mainly affect wireless communication, while microwave weapons can affect all electronics, even stand-alone non-communicating devices. Common to both forms of attack is that the effect is local within its range, which can vary between a few metres and several kilometres.

EM attacks strike at the hardware in electronic systems, in contrast to cyber threats, which attack software in digital communication systems. Note that other technological systems may depend on a system that is impaired by an EM attack, which can be very serious and lead to cascade effects spreading through society. For example, water distribution and traffic signals fail if electric power distribution is interrupted. Hence, particular attention should be paid to dependencies between different vital societal systems.

Among potential antagonists who may use EM threats are foreign powers, terrorists and criminals. A civilian society, which, for its vital functions, relies on wireless communication and satellite-based navigation systems, such as GPS and its European counterpart Galileo, is highly vulnerable to modern electronic attacks in a military conflict. The introduction of the Internet of Things (IoT) will most likely further increase this vulnerability.

Society's increased dependence on electronics and communication

The scenario above could occur since all sectors of society have undergone a rapid development of electronic equipment for the control of various functions, data processing, and communication during recent decades. At the same time, advanced commercially available jammers have emerged with the capability to jam several frequency bands simultaneously, although such devices are illegal to possess or use in Sweden. Several countries are developing microwave weapons, which can disturb or physically destroy electronics. These threats to Sweden's civil defence are more tangible today than during the Cold War.

Military systems have often been equipped with protection against these types of effects, while civilian electronic devices are usually completely unprotected. Electronic Warfare (EW) emerged during the twentieth century as a means to achieve information superiority in military conflicts. EW consists of electronic surveillance (listening to an antagonist's signals, communications, and unintentional radiation from equipment), electronic attack (radiating EM energy to jam or confuse an opponent's electronics), and electronic protection (methods to reduce the effects of an opponent's EW operations). Military powers have spent decades developing methods, technologies and systems to cope with EW, not least for the protection of their own electronic systems and support functions.

The rapid development of electronics during the past few decades, with an enormous increase in computer control and wireless communication, both between humans and between machines, has resulted in many societal functions being based on this technology. Examples include the control and regulation of industrial processes and society's infrastructure via wireless networks, verification of entry permissions at vital plants, issuing warnings over radio and via SMS, payment systems, etc. The digitalisation of our society is progressing within all sectors, even critical services. This makes society dependent on the operation of electronics while at the same time there have been no incentives to introduce protection against antagonistic EM interference. Perhaps this is due to a lack of awareness of such threats to their own systems among those responsible, or not having deemed them as serious or probable, and hence in the short-term the most cost-effective solutions have been chosen during procurement and installation. All commercial electronics must meet Swedish and international requirements regarding immunity to unintentional interference, which can be caused by natural phenomena or by other devices in the vicinity, but these interference levels fall far below the potential of intentional EM threats. Military systems

face tougher requirements on resilience against jamming and interference, which gives much better protection but at a higher cost.

Sometimes electronic equipment is jammed by natural phenomena, such as lightning or solar flares, or unintentionally by other equipment nearby. But individuals with sufficient knowledge can also disrupt societal functions. An example is the Gothenburg riots in 2001, when police radio communication was jammed and false messages were sent. Such disruption is modest compared to the potential of military EW capability. There have also been reports of mobile communications and GPS being jammed as part of Russian EW during the conflicts in Ukraine and Syria.

The total defence concept is central in preparing Sweden to counter many different types of threats. A unified total defence means that civilian actors must consider adopting the same levels of protection as the armed forces. There is currently limited awareness and presence of EM protection within civilian sectors, while the armed forces have long since taken this into account. Increasing the awareness of antagonistic EM threats within civilian sectors is a matter of urgency, so that vital societal functions can be adequately protected.

How to reduce vulnerabilities to EM threats?

The formation of the new Swedish total defence means that many actors will face enhanced requirements for robustness against many different types of intentional or unintentional interference, including antagonistic EM threats. At the same time, the ongoing digitalisation of our society creates new risks of various types of EM interference. If the total defence is designed without this in mind, there is a risk that vulnerabilities will not be discovered and addressed. It is often far more expensive to protect sensitive systems retrospectively than to do so during the procurement or installation phases.

Those responsible for vital civilian functions usually do not have the same knowledge of EM threats and protective measures as is common within the military sector. Awareness of the EM threats faced today needs to increase so that the threats can be incorporated into risk and vulnerability analyses, and identified critical weaknesses can be addressed.

Wireless communication, which is transmitted through air, is much more difficult to protect than communication through metal wires or optical fibres. Hence, wireless communication solutions for vital societal functions need to be resilient against jamming, or have redundancy. This can be realised in different ways, e.g. using frequency hopping regularly or when disturbed; with several

antennas in different locations; with several communication systems using different frequencies; or by supplementing with fibre solutions whenever possible.

Designing adequate protection against antagonistic EM radiation is no easy task. There are several strategies for protecting electronic equipment against EM threats. Depending on how critical the equipment is, and the level of protection selected, the protection can be designed in different ways. With regard to intentional EM threats against mission-critical systems, there are a few general recommendations for consideration:

- Do not spread information about critical electronic systems unnecessarily or information about how they operate, where they are located, and which frequencies are used. An antagonist can use this knowledge in an attack.
- When possible, do not use wireless communication between mission-critical systems. Wired communication is much less sensitive to jamming. Alternatively, equipment with EW protection or redundant systems should be used.
- Make sure that it is not possible to get close to critical systems. Since the effect decreases with distance between source and target, it is beneficial to move barriers and fences, or similar arrangements preventing unauthorised access to critical facilities, further away from the sensitive installation.

Securing access to spare parts and ensuring access to rapid service or repair if a system has been exposed to an EM attack is also a good strategy to help minimise disruption in electronics-based societal functions. It is also possible to enclose critical equipment inside EM shielding walls and to install protective components, such as transient protectors or different types of filters, on connected wires.

It is important to realise that it is not possible to protect all communication and electronic equipment against EM threats. Priority should be given to vital systems, i.e. those whose loss would lead to major disruptions in important services. To achieve this, it is essential to carry out risk and vulnerability analyses, including the risks posed by EM threats to vital systems, on a regular basis. It is always a matter of balance regarding which weaknesses to fix and which level of protection to implement in order to obtain the resilience needed to continue operations when exposed to EM attacks in a severe crisis.

A first step when protecting communication solutions and electronic equipment is to obtain information about existing EM

threats and how to incorporate those into a risk and vulnerability analysis, together with all other identified threats. The next step is to determine whether there is sufficient knowledge in-house to conduct a risk and vulnerability analysis and remedy identified weaknesses, or if external experts are needed. Finally, the analysis should be carried out, suitable protective measures implemented, and regular subsequent verifications that the protection is maintained should be performed. Do not forget the hardware!

12. Artificial intelligence – opportunities and challenges for Sweden's national security

Christer Andersson, Tove Gustavi and Maja Karasalo

Artificial intelligence (AI) is expected to have a significant impact on the development of society over the next few years. AI will be applied in a wide variety of technical systems, which means that AI will also influence vital elements of Swedish defence capability and national security in a broad sense. The question is: are the Swedish authorities, and society in general, prepared to make the most of the opportunities offered by this technology and – not least – to face up to the challenges and threats presented by AI in the new security policy landscape?

Artificial intelligence – a contentious concept

Some would say that artificial intelligence (AI) involves making computers imitate human behaviour. Others consider it to be computer systems that, unlike humans, reason and behave 'rationally' in all situations. There is no universally accepted definition of AI, but generally the term refers to the ability of a computer system to reason sensibly or behave correctly on the basis of information available and previous experience.

In purely technical terms, AI is created by processing information using mathematical methods and logic. Thus, AI is not based on a specific technology but may involve for example statistical methods in addition to various types of machine learning. Machine learning can be described as methods that use available information to train mathematical models of their environment. The models are then used to interpret and analyse the environment. The more information available for training, the more precise models and better analysis results can be anticipated.

Attention has been focused on AI in recent years as certain key technologies have reached such levels of maturity and reliability that they can be incorporated into products and used in society. For machine learning in particular, the maturity of the technology is linked to the development of powerful computers, and to the digitalisation of society which has made large volumes of data accessible to the public. These conditions have helped bring about a development of algorithms and methods that was not previously possible.

AI is a field with no clear boundaries between civilian and military applications. Essentially, a technical system developed to

identify microscopic cancer cells can also be taught to identify bombing targets in satellite images. As much of the technology is freely accessible, it is difficult to obtain an overview of who is using it and for what purposes. The accessibility and dual use bring both advantages and disadvantages from a national security perspective.

AI opportunities and challenges for total defence

Reporting on practical military use of AI is characterised partly by technology optimism, where various successful applications of AI methods are described; and partly by concern for what the development towards more independent technical systems may involve.

For Sweden's total defence, AI methods may lead to improvements in several respects. For the Armed Forces, AI systems may contribute to military operational and tactical advantages, and for the total defence in general, AI provides an opportunity to streamline administrative tasks by introducing different levels of automation.

AI applications

In today's armed conflicts, conventional military warfare often includes elements of hybrid warfare, such as cyberattacks or propaganda campaigns on social media. Thus, analysis of large volumes of data from various domains is necessary to maintain situation awareness. Given this fact, considerable advantages can be derived from the use of AI. Due to the ability to quickly classify and identify patterns in large data volumes, AI technology is well suited for use in sensor data processing and intelligence analysis.

In military sensor systems, AI enables simultaneous and integrated analysis of different types of sensor data, such as radar signals and sonar data, and supports the ability to draw conclusions at high speed. Data processing results can either help the AI system to take independent action or be used to create decision guidance and recommendations for human decision makers. For instance, in a conflict where large numbers of sensors interact with multiple weapon systems, AI systems can help to supply an updated general overview of rapid developments. In today's combat situations, where the need for rapid decisions are constantly on the increase, the ability to quickly analyse large data volumes may be a crucial survival factor.

In intelligence applications, AI offers an opportunity to identify the unexpected – the so called 'black swan' – by analysing large volumes of traditional intelligence data in combination with open web data. With the amount of data produced today, traditional

analysis methods fall short. Processing of data is therefore frequently limited to a known context and a subset of the available data. As a result, the chances of detecting unforeseen incidents are reduced. History has provided us with a number of examples where intelligence efforts have failed to predict forthcoming incidents in time, including the attack on Pearl Harbor and 9/11. AI has the potential to enhance security policy analyses by facilitating detection of both rapid and lengthy sequences of events. With AI, less obvious information or even information that appears to be irrelevant at first glance can be included in the analysis.

AI could become a powerful tool for improving and developing the capability of a range of functions within Sweden's total defence. For the Swedish Armed Forces, AI could offer quality and efficiency enhancements in terms of sensor data analysis and the handling of complex command and intelligence operations. In other parts of the total defence, AI could – for example – be used to detect variations in network traffic that could indicate ongoing cyberattacks on critical infrastructure such as power and water supplies. The scope of potential applications, coupled with the potential for improvement, makes AI technology attractive for financial reasons as well. However, know-how and human resources are needed if the opportunities are to be brought to fruition.

Managing new vulnerabilities

As AI development progresses, there is growing concern in society as to what this technological development entails in terms of reduced transparency and control of autonomous and intelligent systems.

There are plenty of examples of how 'intelligent' systems that usually produce good results sometimes make remarkable errors. One example involves an automated system from Amazon, which had been developed to evaluate job applications. The system had been trained to analyse applications, but after a period of use it was found to discriminate against female applicants. The reason was found to be that there were so few CVs from women in the data used to train the system that greater precision was achieved during training if these applications were rejected. This unwelcome outcome highlights one aspect of machine learning that is important to bear in mind; the behaviour of the system will be governed by the data used to train it. If training data fails to reflect the desired system behaviour, AI-based systems will occasionally make unexpected and sometimes extremely inappropriate 'errors' which could have serious consequences in security-sensitive contexts.

Besides accidental errors of this kind, there are examples of how AI systems can be manipulated by hostile stakeholders. Studies have shown that with knowledge of how a particular AI method works it is possible to manipulate the method so that the AI system gives incorrect answers. For example, by applying subtle pixel-level alterations to an image – alterations which would be unnoticeable to a human observer – one could cause an AI system to misinterpret the image content completely. Furthermore, it has been demonstrated that image recognition systems designed to identify road signs of various kinds can be manipulated to incorrectly interpret a sign if a certain sticker is applied to it. One important aspect of the vulnerability problem is that a great deal of AI technology is openly available. This means that the latest methods for exploiting vulnerabilities in AI systems may be available also for terrorist organisations and criminal networks.

In the light of examples such as those outlined above, there is an ongoing debate concerning the ethical aspects of AI use. One debated topic is the accountability for decisions made and actions implemented by AI-based systems. A key issue in this regard is how to ensure that AI systems work reliably and intelligibly. AI safety is a growing research field investigating issues such as:

- Transparency – how should intelligent systems be designed in order to make them transparent and interpretable by humans?
- Well defined objectives – how can it be assured that the objective defined for an intelligent system will actually result in the desired system behaviour, with no harmful side effects?
- Robustness and stability if conditions change – how can it be assured that unexpected changes to system conditions (power failures, communication problems, etc.) do not result in serious adverse effects?
- Managing vulnerabilities – how should systems be designed and trained in order to minimise the risk of misjudgements due to deliberate manipulation?

In applications linked to defence and security, it is – quite reasonably – more critical than elsewhere that AI systems work robustly and with no adverse side effects. In many military applications, it is also crucial for systems to be transparent so that decisions that have been made can be tracked and explained. As AI offers major benefits, it must be assumed that the technology will nevertheless be used in both military systems and vital societal functions such as electrical power distribution, healthcare and financial trading. Therefore, knowledge of the vulnerabilities of the technology, and

of contingency measures for dealing with potential incidents, are necessary elements of Sweden's total defence.

Premises for Sweden in a changing world

In 2017, Vinnova[3] conducted a study into the development and potential of AI in Swedish industry and society. This study concluded that Swedish AI research currently offers 'limited international competitiveness'. It refers to inadequate investments in AI by companies of all sizes, a lack of government control and a brain drain of AI talent. However, the study emphasises that Sweden has a technology-friendly population, outstanding technical expertise, a well-developed innovation infrastructure, and that the country is at the forefront in terms of IT and digitalisation. Hence, essential prerequisites are in place for Sweden to become a more important AI stakeholder.

One alarming conclusion of the report is that 'other countries are investing more money, faster than Sweden'. In the long term, this kind of development could have major consequences for the competitiveness of Swedish industry; and for national security as well. Countries at the cutting edge of AI development will be able to adopt a position of information superiority, which could alter the security policy landscape. Internationally, China distinguishes itself by making major investments in AI. Countries more on par with Sweden are also investing actively in AI development. Examples of this include France, which in 2018 launched an AI initiative worth more than SEK 15 billion up to 2022; and Finland, which in 2017 became the first EU nation to develop a national AI strategy. In Sweden, the single largest AI initiative is the Wallenberg AI Autonomous Systems and Software Program (WASP), where SEK 1 billion is specifically reserved for AI research. However, WASP is a private initiative funded by the Knut and Alice Wallenberg Foundation. The WASP programme cannot be expected to cater to the interests of the Swedish government, but should rather be viewed as a complement to government initiatives.

The conclusions drawn by Vinnova imply that the Swedish defence sector – both authorities and the defence industry – is in a good position for introducing more AI-based systems. It is worth noting in this context that in combination with other technology, AI could have a significant impact on what has long been one of the major challenges facing the Swedish Armed Forces; namely surveillance of a vast and, in parts, very sparsely populated territory. The extensive coastline in particular presents a challenge from a defence standpoint. Autonomous watercraft

[3] Sweden's government agency for innovation.

and submersibles in combination with intelligent sensor systems could help to improve border surveillance conditions.

Specialist expertise is needed to enable Sweden's total defence to embrace and deploy AI technology. At the same time, the overall knowledge of AI needs to increase within related organisations. AI specialists are greatly in demand on the civilian market, and thereby hard to recruit to the public sector. If maintenance of competence issues are not resolved, it may impede the transfer of AI technology to defence authorities, and the knowledge gap between public and private sector may widen even further.

In addition, both Swedish companies and public authorities are competing on a global market, where large pay gaps between nations can lead to brain drain from nations that cannot offer competitive pay or attractive working conditions. To avoid a future where Sweden's national security is entirely dependent on foreign experts, action must be taken to develop and maintain domestic expertise in advanced data processing.

AI skills key to Sweden's national security

For the total defence to be able to benefit from the opportunities offered by AI technology, and to address the challenges, the AI expertise within relevant organisations needs to increase. Securing maintenance of competence in a field that is evolving rapidly, and that is widely exposed to international competition, is a significant but important challenge for Sweden. Another major challenge for the total defence and society in general is learning how to respond to the new vulnerabilities inherent in AI. Sweden is in a strong position to address these challenges, but relying too heavily on industry and private research initiatives taking responsibility for issues of national interest is a risky strategy.

13. Fake news images and genuine resilience

Niclas Wadströmer, David Gustafsson and Patrik Thunholm

Nowadays, foreign powers can create and distribute virtual images and videos as 'evidence' of fake news. Such images are difficult to distinguish from genuine photos. Advances in artificial intelligence have made it possible for anyone with a computer to create what look like real videos. Moreover, the digital information environment has altered the media landscape and criteria for distribution of information. This presents the Swedish total defence with a new challenge in its efforts to counter opportunities for foreign powers to engage in information influence operations. The total defence also has to safeguard the freedom to form opinions, which is at the very heart of democratic society.

Information influence operations

Imagine a video clip appearing in your social media feed that shows a press conference where a person in authority is describing a serious event. This clip has already been shared thousands of times before it reaches a media house that starts to investigate its authenticity. A reporter gets in touch with that person in authority, who firmly denies that the press conference has even taken place. The reporter believes that what he sees and hears in the clip are proof that the press conference has taken place, and wonders why the person is denying everything. He also asks the person how the clip came to be shared on his social media channel, and how the message was distributed using his official email address. There is complete and utter confusion. After a while, it becomes clear that this viral news clip is fake and that the digital communication pathways of the person in authority have been exploited to underpin the deception. Nevertheless, social media continues to speculate about the authenticity of the video. Can the media house investigating the clip really be trusted? Much later, it is revealed that the person who produced the fake video and hacked the accounts wanted to reduce public confidence in the reporting of news by blurring the lines between what is genuine and what is fake.

The scenario above illustrates how Sweden could be influenced and manipulated or exposed to cognitive stress by a single individual; but also by a foreign power, without the country being at war.

Hundreds of thousands of videos are published on YouTube every day. These include many examples of how actual photos and videos can be manipulated, and how photos and videos can

be completely generated by a computer but still look real. These examples include a video clip showing a computer-generated newsreader who is barely distinguishable from a real person. Another example is a video showing what appears to be former US President Barack Obama making an unexpected statement. In this case someone has recorded a text, transformed the audio so that it sounds like Barack Obama and altered the facial movements in an existing video of the former President so that they match the words recorded.

Researchers at Nvidia have collected many thousands of profile pictures from the Internet and used machine learning to create a program that can generate high-resolution profile pictures that appear to be photos of real people – but none of these people actually exist. These video clips are the result of recent advances in artificial intelligence (AI) which have made it possible to produce moving media, allowing any message to be presented by any person in any location.

Manipulated images

There are many historic examples of manipulated images of reality. Retouching images has been possible for years, although skilled artists were required to make the photos credible.

The film industry has been making animated films for years, and these have become increasingly lifelike as computers have become more widespread. Now we have feature films involving the creation of virtual images of people who are unwilling or unable to participate in the actual filming.

Virtual images are images that look like photographic depictions of reality, but which were actually created entirely or at least partly by a computer. The image appears to show something that genuinely exists, but it is an illusion created by a computer. And it is difficult to distinguish these virtual images from actual photos of real things.

A great deal of expertise and extensive resources are still needed to make feature films using computer-generated characters. That said, technology for creating and manipulating images containing faces is becoming increasingly accessible. Apps that can replace one face with another can now be downloaded with ease. All that is needed is an ordinary computer. Not even particularly in-depth knowledge is required to produce images of surprisingly good quality.

Altered media landscape

The digital information environment has become an important arena for warfare. The relevance of the old notions, that war is

played out between armies on battlefields, has diminished and it is important that the psychological defence tis able to identify, analyse and address influence operations from foreign powers. To succeed in this, information on what can be achieved with modern technology is required.

Most Swedish people are online every day, and their media habits have undergone major changes with the help of mobile technology such as smartphones. Nowadays we can take on the traditional role of viewer, listener and reader, or we can switch to a more active role where we produce and distribute our own content. At the same time, this development has made it easier for foreign powers to use new psychological techniques to influence our perceptions, attitudes and behaviours in order to achieve specific objectives. These objectives could include influencing public opinion and democratic decision-making by undermining decision-making capacity or manipulating opinions.

If a foreign power wanted to reinforce its own position while also weakening Sweden and Swedish interests, it could potentially distribute information of varying authenticity in the information environment. They may report incidents that have never occurred – such as abuse and assaults in known surroundings, or police brutality against minorities – with a view to encouraging polarisation and dividing a country from within. One thing these threats all have in common is that they are aimed at or exploit values vulnerable by their very nature, such as democracy and freedom of expression; along with the fact that antagonists often use new technology.

New technology makes it possible to produce fake news images with ease, rendering it difficult or impossible to trace them back to whoever created them. For instance, images may be distributed anonymously over the Internet or using a stolen digital identity. All in all, the potential for deniability is high. Moving images now have to be regarded with scepticism as a result of the recent development of machine learning. In future, 'putting words into somebody's mouth' will take on an even more literal meaning.

Machine learning

Machine learning, a subfield of artificial intelligence, has made great advances with artificial neural networks (ANNs). ANNs are a software structure inspired by biological brains. ANNs learn from many examples of input and output data, instead of being programmed with explicit rules on how to obtain output data from input data. Deep learning are ANNs with the ability to represent information in hierarchical layers. Google, Amazon, Facebook and other stakeholders with access to enormous

numbers of images with associated captions can teach computers not only to understand the image content, but also to edit and create virtual images. It is possible to change a landscape photo from winter to summer automatically. A sketch drawn by a person can be converted into an image that looks like a photo of a real landscape. It is possible to replace a face, add or remove a person. It is possible to create synthetic video featuring a person that is very difficult to tell apart from an authentic video.

Machine learning involves allowing a machine to learn from examples. You may want to create a program to make portrait pictures, for instance. To do this, you give the computer a large number of examples of portrait pictures and allow the machine to identify special features that are typical for portrait pictures. The machine can then create random images containing these features. Before machine learning came into being, an engineer would have had to identify special features typical for profile pictures and then write a program that created random images with the specified features. Modern machine learning algorithms mean that in many cases, computers are better than engineers when it comes to identifying relevant features.

Generative methods produce more lifelike images

Generative methods can create synthetic images, text and audio – media content created entirely in the computer, that is – without an actual original to work from. Generative Adversarial Networks (GAN), introduced in 2014, is a new generative method which resulted in a breakthrough in the generation of lifelike images. GAN are a further development of Deep learning, which is widely used in AI applications. GAN is trained by means of adversarial training. Two different networks compete against one another: a generative network generates images of a particular type, and a classification network learns to tell the difference between genuine images and generated images. The generative network is enhanced by taking into account features in the generated images that the classification network then uses to tell the generated images apart from genuine images. The classification network acts as a sparring partner for the generative network, and they both go on improving by means of an iterative learning process. As a result, it is becoming increasingly difficult to tell generated images apart from real images. In many cases, the GAN succeeds in creating images that the average person would be unable to tell apart from genuine photos, and even experts may find it difficult to tell the difference.

This capability is becoming increasingly accessible and easy to use. Program code can be downloaded from the Internet, and

advanced knowledge is not needed in order to use it. Programs and pre-trained models for generating images or videos of different types are often freely available to download from the Internet. Nowadays, a small group of people will suffice to create materials of this kind for influence operations, and enormous resources – of the kind that are the preserve of states – are no longer needed. It is also worth noting that private companies have actually published the best research outcomes. There is a lack of transparency here in respect of corporate capabilities and what they choose to keep secret, along with the purposes for which they use this technology.

The total defence

Sweden is restarting its total defence in view of this new technological and digital environment. The Swedish total defence concept encompasses both civil and military defence in a whole-of-society approach to security. As during the Cold War, psychological defence and resilience to information influence operations that threaten society are a prerequisite if total defence is to work. Without social motivation, no part of total defence will function – and nor will the Swedish Armed Forces. Compared to the Cold War, psychological defence measures have taken on greater importance as hostile state actors can now achieve objectives that previously required military operations, simply by using the influence within the digital information environment. Given this fact, it is important for the psychological aspects of the total defence to follow technological development and devise methods that provide genuine resistance to any party wishing to harm us with false images.

Any opponent engaging in information influence operations systematically ensures that vulnerabilities are identified and exploited. There are vulnerabilities in a variety of areas. The modern media system has a number of vulnerabilities in relation to factors such as new technology, new journalistic business models and the increasing number of online news sources. Advocacy efforts have also become more vulnerable as the digital information environment has emerged. With the advent of the Internet, it is easier than ever to fabricate social evidence and incite anger, provocation or upset. Cognitive vulnerabilities may occur due to the way in which the human brain tends to take shortcuts: it is not designed to handle the vast amount of information that it sometimes receives. In this regard, information influence operations can utilise thought patterns and information about us to influence perceptions, behaviours and decision-making processes.

Genuine resilience

The total defence aims to protect fundamental values such as democracy and our self-determination from attacks by foreign powers intent on harming us. Sweden's resilience to these threats is dependent on the agility, digital competence and technical capability of our psychological defence system. This will make demands not only of authorities, but also of citizens, politicians and technology providers.

Ultimately, genuine resilience will be achieved when each and every person adopts a critical approach to images and what they tell us. There is also a need for a general increase in awareness of the opportunities available for manipulating and forging images. Furthermore, research into forensic methods is required so that fake images and systems can be revealed, allowing labels to be attached indicating the origins of images so that anyone viewing such images knows where they originated.

14. How we can protect Sweden's security-sensitive IT services

Anders Elfving and Anton Dahlmark, Fortifications Agency

Protecting vital societal functions is a significant element in the development of the Swedish total defence capability. This is why there is every reason to review the authorities' overall need for physically protected data centres used for security-sensitive IT operations. However, stringent demands in terms of physical protection against weapons effects and IT environment supply system uptime, for example, increase costs and extend lead times. Rebuilding existing facilities versus building new ones must also be weighed up. The changing global political and military dynamics and our insight into the vulnerability of our digitalised society mean that a national initiative in this field is a significant but necessary investment for society and its total defence.

Rapid digitalisation advances result in vulnerabilities

How the digitalisation of our day-to-day lives has made everything simpler and changed our behaviour can hardly have escaped anyone's attention. Large volumes of data generated are frequently processed in cloud services and stored in data centres over time. The fact that these services continue to work 24 hours a day, with no disruptions, is generally taken for granted. The debate regarding our increased vulnerability on account of the digital revolution is ongoing, and there is increasing insight into the potential gravity of the consequences in the event of any issues such as attacks or power failures.

While the topic of IT security is now high on Swedish authorities' agendas, physical protection of governmental IT services has also been identified as a crucial area for review if we are to strengthen the total defence. In 2017, the Swedish Post and Telecom Authority was commissioned by the government to prepare a proposal for a national management model for protected data centres. By no means all data requires enhanced physical protection, but some data is security-sensitive and needs to be protected to prevent both intrusion and military attacks.

Existing or new facilities for data centres?

Secure data centres may be located in protected underground facilities (in rock caverns) or secure buildings above ground. Protected underground facilities have the physical barriers to

protect against weapons effects, but they also protect the data centre's functions and supply systems by offering what is known as fortified protection. Secure buildings above ground are designed with security-enhancing features that prevent or hinder damage to their functions, but they do not have the same fortified protection as underground facilities. The prior period of global stability and cuts in defence expenditure have resulted in protected properties such as underground facilities being taken out of service. This is why authorities in recent years have been asking whether these could be used for protected data centres, or whether it would be more appropriate to build new protected facilities.

One common perception is that implementation of protected data centres in underground facilities is straightforward. The usual arguments claim:

- That a large number of empty underground facilities are available that could be used as data centres following minor refurbishments – and that this would be relatively inexpensive to implement.
- That underground facilities automatically provide protection against weapons effects of all levels and types.
- That while retaining fortified protection, underground facilities can easily be adapted for data centres consuming ten megawatts (MW) or more – equivalent to the power produced by about six wind turbines or the power required to run more than 4000 homes.
- That underground facilities are within 15 to 20 km of the geographical locations of current operations. That data centres can be established quickly at existing underground facilities.

Besides the above expectations, high uptime levels are frequently required as well. In other words, how much of the time facilities are operational and delivering the intended capability is also a factor to consider. Uptime is generally higher with redundant systems, but these are often more costly than anticipated.

However, the actual situation is not quite the same. Few of the underground facilities available would be suitable for use as data centres, and those that do exist are rarely located close to population centres. There is frequently a significant need for decontamination and extensive investment before the facility can be commissioned. Maintaining fortified protection while also devising a solution for the necessary cooling of the IT environment presents a major challenge. Although the rock has mostly been removed already, adaptation work takes longer than anticipated. However, the

procurement time is considerably shorter when refurbishing a vacant underground facility, compared with constructing a new facility.

When building from scratch, the fact that the facility is designed for use as a data centre right from the outset is an advantage. There are economic benefits to be derived from coordinating physical protection, construction costs and operating costs when allowing multiple social stakeholders to share a single, physically protected facility. However, there are also negative aspects to sharing facilities. If only a small number of facilities are established as a result, there is a risk of them being viewed as more high-value targets from an attacker's perspective, compared with a large number of attack targets over a wide area. There is therefore a risk of more far-reaching consequences of an attack on a high-value target.

Power supply with no failures

The need for a robust power supply is another aspect to take into account. Data of significant importance to society must be stored and managed without power failures. IT services are also power-hungry applications requiring an efficient cooling infrastructure. Without cooling, IT equipment overheats – sometimes within minutes – and disables the facility's functions. The large amounts of energy that need to be dissipated from data centres mean that water cooling is deemed to be far more efficient than air cooling or geothermal cooling. It is therefore appropriate to select physical locations adjacent to large reservoirs or watercourses, which of course limits the number of potential locations.

Society is currently making a transition to fossil-free energy. At the same time, Svenska kraftnät[4] indicates that the need for auxiliary power supplies is increasing. A reliable, dependable auxiliary power supply is absolutely essential in a number of sectors of society that are crucial to maintaining a functional total defence: county councils, municipalities and voluntary organisations, for instance. Auxiliary power supplies at present usually involve diesel power stations, but these have a number of limitations: (i) major environmental impact, (ii) problems with fuel distribution during crises, (iii) dependency on imports from other countries, (iv) high thermal signature during combustion, making facilities easier to detect, and (v) noise.

All in all, therefore, it is necessary to test alternative new energy solutions to provide reliable auxiliary power supplies at vital societal facilities such as future data centres. Battery and fuel cell

[4] Svenska kraftnät is a Swedish state-owned electricity transmission system operator.

technologies are examples of areas where recent development has shown promising results from a robust societal perspective. For protected data centres, it is particularly important to ensure that the auxiliary power supplies of the future are not only robust, but also easy to maintain and inexpensive to run. Moreover, power and cooling supply intakes must be protected from the pressure waves caused by bombing attacks, threats from electromagnetic pulse and high-power microwave attacks and other threats. This may present a challenge, however, as these intakes often have to cover large areas.

Varying uptime and security requirements

The basic functioning of society is rarely dependent on a single stakeholder's ability to provide a service under difficult conditions. Electricity, data and telecommunications, financial services, transport, fuel distribution, food supply – everything is interlinked in various intricate chains of dependency. If the function offered by a social stakeholder fails – if an IT service is disabled, for instance – this may impact on all parties who are dependent on this service in their turn. Society would benefit from maintaining a holistic approach with regard to the uptime of individual subfunctions, along with selected levels of protection and the extent to which they merit protection.

Table 1. Assumed need for uptime and requirements for various IT services at different times

	Peacetime	Crisis	War
High uptime	Greater need	Average need	Reduced need
Secure building	Greater need	Greater need	Average need
Protected facility	Reduced need	Reduced need	Reduced need

Demands for higher levels of protection and uptime are very much cost-driven. The cost of a data centre increases rapidly depending on the level of uptime, potentially resulting in a highly costly undertaking. It is reasonable to assume that most vital societal IT facilities will have varying demands in terms of uptime and security, and that these may vary during peacetime, times of crisis and war. A more in-depth analysis is of course necessary, but a likely scenario is that a large number of IT services will have high uptime requirements in peacetime and considerably reduced requirements in wartime, when only the most essential functions are expected to be operational. In peacetime, the number of IT services requiring secure buildings above ground is likely to be

considerably higher than the number of IT services requiring protected underground facilities. Table 1 shows a possible simplified description of this scenario.

According to what in Sweden is known as the responsibility principle for the crisis management system, individual stakeholders such as authorities have the same responsibilities in wartime as in peacetime and make their own decisions on what protection and uptime they need. Issues relating to which stakeholders' activities should constitute protected entities or issues of national interest, which physical threat levels should be addressed and which uptime levels must be achieved by each individual subfunction should benefit from being managed at an overall societal level. The Swedish Post and Telecom Authority's proposal for a management model in respect of protected data centres may present a useful starting point. This proposes the following:

- **Priority function.** A governmental function tasked with classifying and prioritising protection needs for the IT services of security-sensitive operations from an overall societal perspective.
- **Facility administrator.** An organisation that operates on the basis of the proposed administration model to manage the portfolio of protected data centres.
- **Facility owner.** An organisation that owns and manages the facilities that have protected data centres.
- **Occupants.** Practitioners running security-sensitive operations that need to house all or parts of their IT environments in protected data centres.

How could a governmental data centre concept be structured?

Protected facilities with a high useful power output – that is, a power output that is useful for the facility's functions – are expensive and take a long time to build. That said, facilities with high levels of fortified protection are necessary from a total defence perspective. One possible way of balancing the ratio of usage to risk and cost for a protected facility would be to implement less stringent requirements in terms of high useful power output. The outcome would be a less complex design at a lower cost. This would also accelerate the procurement process. Moreover, it may also make it easier to close in on the environmental quality objectives, as well as improving sales of surplus heat.

In most respects, secure buildings should be constructed so that they are as similar as possible to modern commercial data centres. Principles and experiences should be 'recycled' and developed

in order to gain synergies as future expansion of a national data centre concept progresses; but they can largely be repeated in new locations in terms of design and capacity. However, one crucial difference between secure buildings and commercial reference properties is that physical security aspects will cost more, as it is imperative to protect the data centre from peacetime threat scenarios; including burglary, sabotage, suicide bombers, attacks with guns, car bombs and ramraiding.

It is likely that stringent demands are made of physical security for the vast majority of IT services that may be considered for a governmental data centre concept, but not on the level offered by protected underground facilities. On the one hand, a secure building that is specifically planned, positioned and designed for the purpose will probably offer an entirely satisfactory level of physical security for the majority of vital societal IT services. On the other, however, a wide range of IT services also have to survive the demands of war by means of the fortified conditions offered by protected underground facilities.

Another way to derive benefit from a protected underground facility is to use it for storage and backup purposes; which is a less energy-intensive undertaking on the whole. Energy-intensive server services with more stringent uptime requirements can primarily be managed in secure buildings. This ensures that high capacity is available for vital societal IT services in terms of uptime and extensive security on a day-to-day basis, while the overall data volume is backed up regularly to a protected underground facility. In the event of adverse incidents, this concept means that data backed up to a protected underground facility will be inaccessible while it is being recovered to another secure building that is operational, but on the other hand it will be highly accurate in that no data will be lost and so it will be possible to recover it.

A PROTECTED UNDERGROUND FACILITY AND A SECURE BUILDING – AN ADVANTAGEOUS COMBINATION

There is need for further examination of protected underground facilities from a strategic perspective. Nevertheless, as a final example below, an overall national power requirement slightly in excess of 20 MW (enough power to run around 9000 homes) can be achieved by using 15 buildings and protected underground facilities (new sites and converted rock caverns) all over Sweden:

A conceptual regional data centre cluster could be distributed as follows:

- Two secure buildings, each with a power output of 2 MW (new sites)

- One protected underground facility with a power output of 0.5 MW (conversion of an existing underground facility that is currently not operational)

Five such regional data centre clusters throughout Sweden would therefore involve, in total:

- Ten secure buildings, each with a power output of 2 MW (new sites)
- Five protected underground facilities with a power output of 0.5 MW (conversion of existing underground facilities that are currently not operational)

As mentioned previously, the relatively long procurement time for a data centre concept is worth noting. Time-critical parameters that influence the production time for a new secure building include acquisition of land, environmental surveys and a secured contractor procurement process.

It is estimated that it takes about two years to procure a secure building. It is thought that conversion of a fortified underground facility will take four to five years. Several regional data centre clusters can be constructed by degrees or simultaneously. However, it is fair to assume that there will be no need for the full capacity in the short term, and that there will therefore be no need to implement the entire concept in parallel. Making the most of experiences from initial construction projects before taking unnecessarily large steps is also logical. It is therefore reasonable to assume that a total procurement time of about ten years may be required.

Overall, a potential data centre concept as described in the example above may offer high levels of uptime and redundancy at a more reasonable cost than if all the data centres are newly constructed fortified underground facilities. Although uptime for vital societal and security-critical IT services will be affected with the data centre concept, this will provide a high level of security in terms of both physical perspectives and accuracy, in the sense that no data will be lost even under extreme conditions such as times of crisis or war. However, a prerequisite for a procurement time of around ten years is that necessary strategic elements such as requirement specifications, funding and organisation have been established beforehand. Hence decision-makers should raise awareness of the needs and challenges associated with national coordination of protected IT services so that the process can commence. This is a vital and necessary investment in the future for the total defence of Sweden.

15. FOI and the needs of the total defence

Eva Mittermaier

Strategic Outlook 8 highlights important perspectives with regard to technological and global development, as well as related challenges. There is a major need for continuous and coherent development of knowledge if the Swedish total defence is to be able to deal with these changes, including the new threats faced. FOI has developed a model relating to perspectives on knowledge development in order to meet the needs of the total defence. The aim of this model is to facilitate discussion among various authorities and other total defence stakeholders.

FOI's knowledge model

The new total defence has some major knowledge requirements involving many different fields. Knowledge relating to different security threats and ways of dealing with them provides a fundamental starting point for both the crisis management system and the total defence. Frequently, this knowledge is highly specific and requires both basic and applied strategic research in a number of different fields; the spread of viral diseases, extremist propaganda in social media and the interpretation of nuclear weapon doctrines, for instance.

If the development of knowledge about threats is to have the desired effect in the development of the total defence, it needs to be made available in the vital societal functions where the knowledge is to be applied, such as healthcare, payment systems and power supply systems. This is by no means a simple task as it involves many different stakeholders such as authorities, municipalities and private industry, from a wide range of sectors with different prerequisites, needs and roles.

The figure below presents a model that includes areas of knowledge to meet the needs of the total defence. The model was originally designed to provide a platform for FOI's ongoing total defence efforts, allowing FOI to clarify – in discussions with principals – specific fields in which FOI could make contributions. However, the model can of course also be used as a more universal foundation for discussion with regard to the knowledge needs of the total defence. The model illustrates four different knowledge layers.

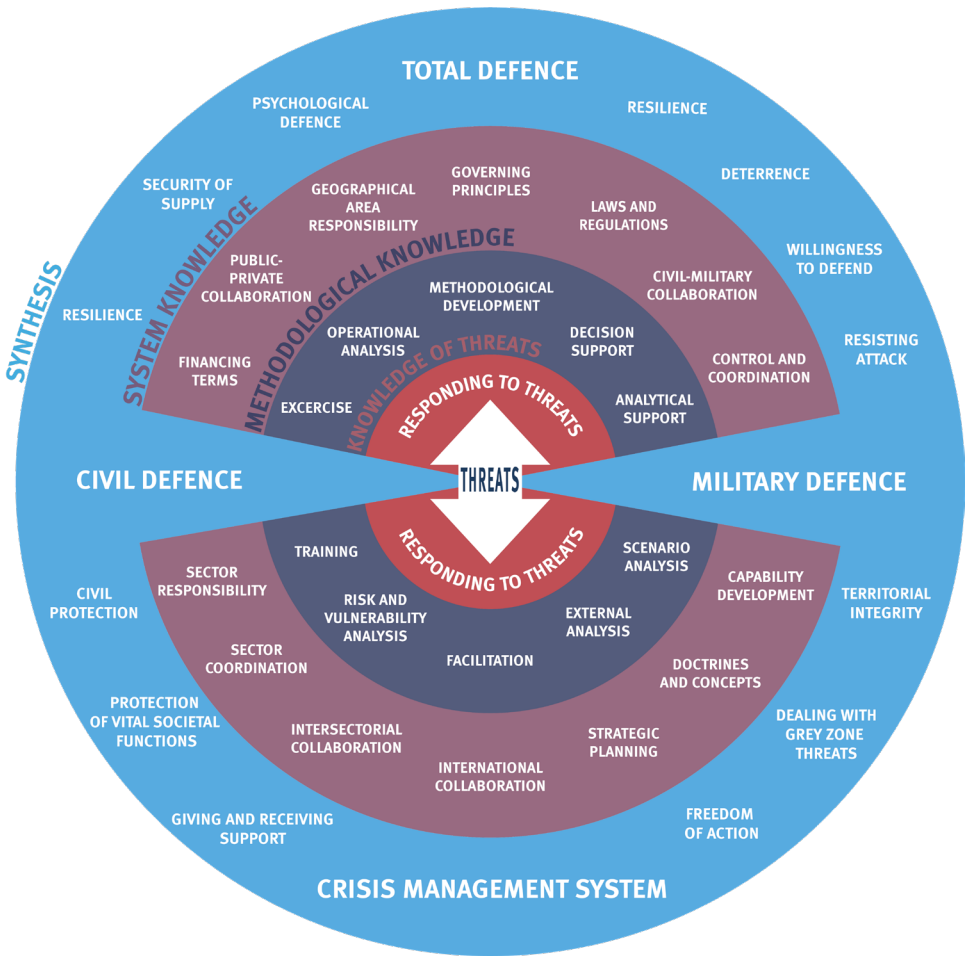

Figure 1. A model for building knowledge for a changing total defence.

Knowledge of threats – the first layer

Identifying, understanding, analysing and responding to antagonistic threats involves fundamental expertise and cutting-edge competence on threats and adequate countermeasures. Knowledge of threats, for example, comprises information security and cyber issues, as well as military threats and protection against conventional weapons and hazardous substances (chemical, biological, radioactive and nuclear). Potential vulnerabilities resulting from technological development also have to be considered as threats.

Threats also include influence operations, terrorism, sabotage and organised crime, for example, when what are known as 'grey zone threats' are included in the total defence perspective. It is all a matter of finding ways to protect people, societal functions, soldiers, military systems, civilian infrastructure, property, social systems, values, etc. Knowledge of threats also involves ways of analysing individual threats and how these can be handled. Methods include modelling, simulation and metrological methodology.

Methodological knowledge – the second layer

Methodological knowledge involves supporting analysis and decision-making processes in various ways, thereby reinforcing the abilities of the relevant total defence stakeholders to identify and respond to threats. This involves knowledge on how to support others, making it possible to build up and utilise knowledge held by other stakeholders, or together with them: in others words overall methodological knowledge.

This knowledge is required in scenario methodology and gaming, for example, where scenarios are used to describe threats and develop the utilisation of expertise through emergency response planning in the various sectors and functions of society. Vulnerabilities can be identified and managed by examining them and attempting to devise appropriate measures. This may involve risk and vulnerability analyses, scenario exercises where participants can identify and discuss vulnerabilities, identifying which stakeholders need to work together in order to respond to threats, or identifying which command and control systems are required for the stakeholders involved to be able to work in a coordinated fashion. It may also involve looking at how stakeholders can work together to exploit information from existing technical sensors and other data in order to achieve enhanced operational situation awareness, allowing them to communicate robustly with one another.

System knowledge – the third layer

System knowledge comprises an overall understanding of the system in which knowledge of threats and methods are to be used, such as in policy development and strategic planning, doctrine and concept development and capability development. System knowledge also includes the prevailing criteria in these contexts: responsibilities, funding conditions and various forms of coordination and collaboration, for instance.

Synthesis – the fourth layer

Coherent total defence requires coherent development of knowledge. Synthesis includes knowledge relating to the various elements of the total defence that affect the prerequisites, objectives and key tasks of the crisis management system, civil defence and military defence. Knowledge on how important sectors of society actually function in practice is also required in this regard.

This knowledge layer also includes an understanding of how security and defence policies influence the total defence, as well as the ability to identify specific needs for the total defence; which in turn may require new research and long-term technological and concept development.

Knowledge development for a coherent total defence

In conclusion, it needs to be possible to integrate the four different knowledge layers in order to guarantee the development of an appropriate and coherent total defence, regardless of where this knowledge is actually developed. Both methodological and system knowledge are required in order to utilise specialised knowledge of threats in the various operations and development processes of the total defence. FOI's ambition and objective is to continue supporting the various elements of society by providing expert knowledge, analyses, decision support and strategic decision data – which covers all the knowledge layers.

Biographies

Christer Andersson, Licentiate of Engineering, Scientist and Analyst at FOI's Department of Underwater Technology. He works in various development projects for the Swedish Armed Forces regarding technical threat scenarios to strengthen Swedish military capabilities and capacity. Christer has broad international experience from both civil and military activities, with a focus on image information retrieval and as an expert for various organisations.

Maria Andersson is a Senior Scientist at FOI's Department of Sensor Informatics. She is also an adjunct senior lecturer and docent in energy systems at Linköping University. Her areas of expertise are methods for automatic detection of critical information in large data sets as well as systems analysis for cooperation between actors.

Samuel Bergenwall is a Senior Analyst at FOI. He works at the Department of Security Policy and Strategic Studies, where he currently leads a project for long-term analysis of global trends. During his time at FOI, Samuel has mainly worked on issues related to security in Asia and in the Middle East.

Åsa Berglund is a legal expert and advisor at FOI, where she mainly works in public law. Her areas of expertise are public access to information, secrecy and confidentiality as well as personal data issues. Since 2018, she has been FOI's data protection officer. Previously, Åsa has been part of the legal staff at the Swedish Armed Forces.

Anton Dahlmark is Director of Development and Head of the Development Department at the Swedish Fortifications Agency. He has worked in the area of protection and construction technology for protected facilities since 2010. Previously, Anton has worked for the Swedish Armed Forces and in crisis management.

Carl Denward is a social scientist and a Senior Analyst at FOI's Department of Societal Security and Safety. His area of expertise is the civilian part of Swedish preparedness, i.e. civil defence and crisis management, focusing on strategy and policy issues. Previously, Carl has worked with preparedness issues at a municipal level.

Fredrik Ekström is a Biochemist and works as Research Director at FOI, Department of Organic Chemistry and Life Sciences.

Anders Elfving is a Research and Development Coordinator at the Swedish Fortifications Agency. Previously, he has worked as senior researcher at FOI's Department of Weapon Effects and Security of Explosives. There, he managed several research projects related to detection of explosives as well as harmonisation of certification processes for security products. Anders has a PhD in Materials Physics at Linköping University and has a background in the development of semiconductor-based micro-sensors.

Carina Gunnarson is Senior Researcher at FOI's Department of Security Policy and Strategic Studies. Her research areas include European politics, Africa and organised crime. She is an associate professor of political science at Uppsala University.

David Gustafsson is a Senior Scientist and project manager at FOI's Department of Sensor Informatics. David mainly works with machine learning methods, such as Deep Learning, to analyse images of different modality. He holds a Master's Degree in Computer Science from Lund University and a Doctorate in Computer Science with a focus on image analysis from the University of Copenhagen.

Jakob Gustafsson is an Analyst at FOI's Department of Strategy and Policy and one of the editors of Strategic Outlook 8. He studies transatlantic and northern European defence and security policy, as well as processes of military force generation. Jakob has an educational background in Political Science.

Tommy Gustafsson is a Research Engineer at FOI's Department of Information Security and IT Architecture. His areas of expertise are network security and information security in vital societal functions. He is active within the National Centre for Security in Control Systems for Critical Infrastructure (NCS3), a centre of excellence that FOI operates in collaboration with the Swedish Civil Contingencies Agency (MSB).

Tove Gustavi is a Senior Scientist at FOI's Department of Decision Support Systems. She has a PhD in Mathematical Systems Theory with applications in robotics and has worked at FOI since 2010, amongst other things with the development of technical support for intelligence analysis and with automated data analysis in civil transport security. She was recently project manager for an FOI project that studied defence-related applications of artificial intelligence and was, for several years, visiting researcher at KTH Royal Institute of Technology.

Tomas Hurtig holds a Ph.D. in plasma physics and is Deputy Research Director at FOI's Department of Weapons and Protection. He has worked at FOI since 2004, primarily with research on microwave weapons and plasma physics. He is the project manager for the Swedish Armed Forces project, HPM Vulnerability Analysis, as well as competence area leader for the Protection against Electromagnetic Effects area.

Jenny Ingemarsdotter is a researcher at FOI's Department of Societal Security and Safety with a focus on crisis management, civil defence and total defence. She holds a Degree of Master of Science in Engineering Physics and a PhD in History of Science and Ideas, both from Uppsala University. Jenny has served in many roles at FOI, including as operational analyst at the Swedish Armed Forces and analysis support for civilian authorities. Currently, she is involved in a research project on civil defence in the grey zone.

Bengt Johansson is a Scientist at FOI and Associate Professor in Environmental and Energy Systems Studies at Lund University. His field of expertise is energy and climate policy and in recent years he has, amongst other things, pursued an interest in how energy security is affected by the ongoing transition of the energy system. Bengt has previously worked with energy and climate policy issues at the Swedish Environmental Protection Agency for several years.

Daniel K. Jonsson is one of the editors of Strategic Outlook 8. He is a research director at FOI's Department of Societal Security and Safety. He has a background in energy and environmental research. Daniel has a doctoral degree in infrastructure and community planning and is Associate Professor in Energy Analysis. Daniel leads a research project on civil defence in the grey zone and coordinates FOI's support to the Swedish Energy Agency's total defence planning.

Maja Karasalo is a Scientist at FOI's Department of Decision Support Systems. She works with methods for automatic text analysis and research in the field of artificial intelligence and machine learning. Maja has a Degree of Master of Science in Engineering: Engineering Physics, and is Doctor of Technology in Optimisation and Systems Theory, both from KTH Royal Institute of Technology. She has previously worked as a researcher and system developer in SAAB's data fusion group.

Maria Lignell Jakobsson is Director of Planning at the Director-Generals Management Support Office at FOI. She is responsible for coordinating operations management and other multi-agency processes, external environment monitoring and analysis, and the agency's contacts with the Government Offices. Maria has served in many roles at FOI. Up to the end of the 1990s, she worked with studies in total defence, dependencies and operational capability. Thereafter, she focused on strategy and market issues. She has also been Head of Division for Defence Analysis.

David Lindahl is a Research Engineer at FOI's Department of Information Security and IT Architecture. David's research focuses on protection of critical infrastructure against cyberattacks, as well as the use of cyberattacks in conflict. During the last ten years, he has instructed actors within the total defence, such as the Swedish Armed Forces, government authorities and private companies, on how to respond to cyber threats.

Sara Linder is a Senior Scientist at FOI's Department of Robust Telecommunications. She has been working at FOI since 1998 with research on robust radio communication systems. Her area of expertise is consequences in communication systems from unintentional interference, often referred to as intersystem interference. She also researches techniques to increase the robustness against both intentional and unintentional interference.

David Lindgren is a Senior Scientist at FOI's Department of Sensor Informatics. He has a Doctoral degree in Automatic control from Linköping University. His areas of expertise involve statistical estimation theory, sensor fusion and sensor networks. He has served as head of both national and international projects on surveillance applications.

Jenny Lundén is an Analyst at FOI's Department of Strategy and Policy. Her focus area is total defence where she works with analyses in both civil and military defence. As operational analyst, Jenny provides analysis support in the Total Defence Department at the Swedish Armed Forces. She has previously been a technical analyst in the business sector and has conducted investigations and analyses into renewable energy. Jenny holds a master's degree in physics from Lund University and a PhD in meteorology with a focus on the Arctic from Stockholm University.

Eva Mittermaier is a Research Director at FOI's Department of Societal Security and Safety. Eva has served in many roles at FOI and mainly worked on issues related to emergency preparedness, societal security and civil defence. In recent years, Eva has participated in internal work concerning FOI's possible contribution to the build-up of the civil defence and of the total defence.

Peter Nilsson is a Systems Scientist and Researcher at the Department of Human, Technology Organisation. He works with issues relating to methods for needs analysis, requirements engineering and methodology for system development, primarily through model-based methods and different architectural frameworks. Peter often works closely with other authorities and has participated in several development projects, primarily with the Swedish Armed Forces, but also with the Swedish Police Authority and other agencies.

Sten E. Nyholm is a Deputy Research Director at FOI's Department of Weapons and Protection. He has worked at FOI since 1996, primarily with research on microwave weapons. In addition, his work has involved microwave weapon technology, explosives science, insensitive munitions and various military applications of pulsed electrical energy. He was the project manager for the main study of risk and vulnerability analysis regarding antagonistic electromagnetic threats to critical infrastructure, which was carried out on behalf of the Swedish Civil Contingencies Agency (MSB).

Jonas Näslund has a PhD in Virology from Umeå University and works as a Scientist at the Department of Biological Agents at FOI. Jonas's expert area is viruses with a special focus on viral zoonoses and their vectors, such as mosquitoes and rodents.

Matilda Olsson is an Analyst at FOI's Department of Strategy and Policy, focusing on civil defence and total defence. In recent years she has conducted studies on the role of the business sector and the county administrative boards in the total defence and served as an operational analyst at the headquarters of the Swedish Armed Forces. Matilda has an educational background in Political Science and Sustainable Development at Uppsala University.

Per Olsson is a Scientist at FOI's Department of Defence Economics. His areas of expertise are defence spending and military equipment supply. He is currently working on a report on Sweden's military equipment supply on behalf of the Expert Group on Public Economics (ESO). Per holds a Master's Degree from Lund University.

Sofia Olsson is one of the editors of Strategic Outlook 8. She is an Analyst at FOI's Department of Asymmetric Threats. Sofia focuses on cyber security and serves as analysis support for the Swedish Armed Forces. Sofia has an educational background in Global development studies and War studies.

Niklas H. Rossbach has been Project Manager and Editor-in-Chief of Strategic Outlook 8 since February 2019. He is a Senior Researcher at FOI's Department of Security Policy and Strategic Studies, with US and British foreign policy as his main focus. He also works on energy and security and has written about psychological warfare, specifically Sweden's so-called psychological defence, while a Visiting Fellow at the Changing Character of War programme at the University of Oxford. He holds a PhD in history from the European University Institute.

Per Stenberg is a Senior Scientist at the Department for Biological Agents. Per is a geneticist and works part-time as a researcher at FOI and part-time as research leader at Umeå University.

Anna Sundberg is one of the editors of Strategic Outlook 8. She is a Deputy Research Director at FOI's Department of Security Policy and Strategic Studies, where she focuses on the security and defence policy of European states. Anna is currently serving as analysis support at the Ministry of Justice.

Ola Svenonius, (PhD) is a political scientist at FOI's Department for Asymmetric Threats, focusing on hybrid threats and information influence. Amongst other things, he leads a research project on countering propaganda funded by the Swedish Civil Contingencies Agency (MSB). He also participates in the BEViS project, aiming to generate collaborative solutions for inter-agency sensor data exchange. During his time at the Stockholm University, Ola focused on issues of surveillance, money laundering prevention, and Central and East European politics.

Patrik Thunholm, Master of Philosophy in Information Science, and Master of Philosophy in Jurisprudence, is an Analyst at FOI's Department of Asymmetric Threats. He is a reserve officer in the Swedish Armed Forces with a focus on psychological operations. He is currently on leave of absence from FOI to work as branch head of the EU operation in Mali.

Camilla Trané is part of the editorial board for Strategic Outlook 8. She is a Senior Analyst at FOI's Department of Operations and Exercises. Camilla has mainly worked on applying methods in practice, primarily exercises, appraisal and experience management. In her role as an analyst, she has many years of experience as direct support in these methodologies, both from the civilian and the military side.

Niclas Wadströmer is a Senior Scientist at FOI's Department of Sensor Informatics. Niclas mainly works with image and signal analysis, amongst other things with machine learning methods such as deep learning, for signals of different modality. Niclas has a Degree of Master of Science in Engineering, and a PhD in Image Coding from Linköping University.

Kia Wiklundh, PhD, has previously worked as Deputy Research Director at FOI's Department for Robust Telecommunications. Her area of expertise is robust wireless communication systems. The focus has mainly been on military radio systems, but she has also worked on investigating vulnerabilities in civil systems and has been responsible for FOI's radio communication intersystem interference activities.

Ann Ödlund is a Senior Scientist at FOI's Department of Strategy and Policy. Ann has an educational background in behavioural science and organisational psychology. In recent years, she has conducted studies primarily in total defence and civil defence and has published several reports on the subject.

Josefin Öhrn-Lundin is Project Manager and Editor for Strategic Outlook 8. She works as an Analyst at FOI's Department of Defence Economics, focusing on military equipment supply and logistics. Josefin holds an MSc in Economics of Innovation and Growth from KTH Royal Institute of Technology.

FOI, the Swedish Defence Research Agency, is one of Europe's leading research institutes in defence and security. FOI is a government authority under the Ministry of Defence. Our largest clients are the Swedish Armed Forces, the Swedish Defence Materiel Administration, the Government Offices and the Swedish Civil Contingencies Agency. We also have many assignments from other government authorities, municipalities and companies.

The first edition of Strategic Outlook was released in 2009. Strategic Outlook is a recurring, forward-looking collection of FOI reports, highlighting questions of great strategic importance for policy in the domains of defence, security, and foreign affairs.

This year's edition takes a closer look at the development of Sweden's restarted total defence system.

Strategic Outlook is available for download at www.foi.se.

FOI

ISSN 1650-1942

www.foi.se