Strategic Outlook 7

Perspectives on national security in a new security environment

Cecilia Hull Wiklund, Daniel Faria, Bengt Johansson
and Josefin Öhrn-Lundin (eds.)

FOI-R--4456--SE

October 2017

Strategic Outlook 7

Perspectives on national security in a new security environment

Cecilia Hull Wiklund, Daniel Faria,
Bengt Johansson and
Josefin Öhrn-Lundin (eds.)

FOI

October 2017

FOI-R--4456--SE

ISSN 1650-1942
Printed in Stockholm 2017 by The Swedish Defense Research Agency, FOI
Cover photo: Anton Balazh/shutterstock.com
FOI-R--4456--SE, version 2
Approved by Lars Höstbeck

Table of Contents

Introductory Remarks

Since the publication of the first *Strategic Outlook,* in 2009, the global security situation has changed in a way that has increasingly made our own geographic neighbourhood central to Swedish defence and security policy. This has been accompanied by rapid technological developments in both the military and the civilian fields, which create not only new opportunities, but also new vulnerabilities and challenges for today's decision-makers.

The creation of a safe and secure society requires deep knowledge of a broad spectrum of issues within the areas of defence and security policy, defence planning, military technology, critical infrastructure, information security and protection against chemical, biological radiological and nuclear (CBRN) threats, to name just a few. It is the role of FOI to deliver such knowledge to relevant societal actors. By means of its long history in research and development, FOI has an accumulated competence of almost unique depth and breadth and therefore constitutes a core resource on Swedish defence and security. *Strategic Outlook,* which is one of FOI's signature publications, seeks to reflect this competence in an accessible form while maintaining scientific quality. My hope is that this new edition of *Strategic Outlook* is a stimulating and valuable read both for decision-makers and the interested layperson among the general public.

To reflect the current global situation, the theme of this edition of *Strategic Outlook* is "Perspectives on Swedish national security in a new security environment". The chapters are a sample of FOI research, which reflects in numerous ways the security challenges facing Sweden. The opening chapter highlights the challenges that Sweden is confronting in its transition to a focus on national security, not least on the questions of resource distribution and approach. The chapter is followed by an analysis of defence finance, which pinpoints an elevated level of unconscious political risk-taking in defence and security policy. The geopolitical context is then treated in two security policy analyses. The first involves the Baltic Sea area, which is a region of geostrategic significance in the interaction between Russia and NATO. The second describes the opportunities and conditions for cooperation between Sweden and Germany, NATO's most important member in the Baltic Sea area.

As a result of the increased focus on national security, the concept of total defence and territorial defence have grown in importance for Swedish defence policy. This edition of *Strategic Outlook* discusses total defence from two perspectives. Chapter 5 highlights the key outstanding questions regarding how to build a modern system of total defence that has maximum defence impact: the respective critical defence functions of the Swedish Armed Forces and civil defence; how national authorities should be organised; and the need for long-term decision support. Chapter 6 discusses "psychological defence", an essential function for countering the influence of disinformation and maintaining morale.

The rapid development of information technology creates new challenges for defence and security. This is demonstrated in four chapters for this publication. Digitalization and the use of the Internet for critical societal functions create new opportunities but also new dependencies. Intelligence-gathering, Influence Operations and covert military operations are identified in chapter 7 as areas where the Internet has new significance as a military tool. Chapter 8 discusses how all the various products that are to a growing extent connected to Internet (the "Internet of Things") increase the risk of cyberattacks that would create serious disruption to critical societal systems. The electricity distribution grid is a prime example of such a system, and chapter 9 shows how so-called smart electricity grids increase vulnerability to attacks. Chapter 10 discusses how the growing accessibility of geographical data, facilitated by ongoing digitalization, can make society more efficient, but also adds to the risk that sensitive information could be released in unintended ways.

Technological development produces ever more advanced weapon systems, which Sweden must be able to utilize as well as counteract. Several chapters deal with these complex issues. Chapter 11 enquires into the significance of the presence of long-range weapons in our geographic neighbourhood for assessments of Sweden's defence requirements; chapter 12 argues the need for a Swedish defence and security strategy on space-related issues; and chapter 13 discusses how Swedish decision-makers can be better prepared to deal with serious food contamination resulting from a nuclear attack.

The report concludes with three chapters of a character that is new for *Strategic Outlook.* Authors from Norway and Finland have been invited to contribute their reflections on defence planning in their respective countries. This creates a valuable context in which to view the previous chapters, which primarily present a Swedish perspective. The concluding chapter discusses the importance of defence research to Swedish security, the very factor that is FOI's primary *raison d'etre*.

This *Strategic Outlook* has involved authors from all of FOI's research divisions. In addition to a huge thank you to the authors, I would also like to extend thanks to the four editors who have made this seventh *Strategic Outlook* possible.

Stockholm, October 2017

Jan-Olof Lind
Director General
FOI – the Swedish Defence Research Agency

1. National Defence and the Baltic Sea Region: Sweden's New Focus

Robert Dalsjö and Michael Jonsson

The security situation in the Baltic Sea region has deteriorated over the past decade. A more threatening Russia has led Sweden to shift its focus from the situation in distant lands to its more immediate neighbourhood. National security and national defence are once again on the agenda, but both resource allocation and attitudes remain influenced by the many years in which peace and security could be taken for granted. In addition, the ship of state is slow to turn. The known weaknesses in both Sweden's armed forces and total defence expose the need for urgent measures. Analysis and policy formation are hampered, however, by an unwillingness to openly discuss Sweden's national interests and the growing threats against them. The Swedish national security strategy published earlier this year must be supplemented by clearer objectives, additional financial resources and sharper methods for addressing the vulnerabilities resulting from decades of wishful thinking, underfinancing and insufficient threat-awareness.

From sunshine to storm warning

The decades after the fall of the Berlin Wall was a period of rosy optimism when it was widely assumed that Russia was no longer threatening or dangerous and military power was no longer needed in Europe. Western Europe disarmed, the USA withdrew almost all of its units and the North Atlantic Treaty Organization (NATO) turned its attention to peace-support operations in distant lands.

Sweden also downsized its military defence and adapted it to international missions, while the civilian components of the elaborate total defence concept were simply disbanded.[1] In planning, attention to preparedness issues vanished since these were considered outdated and irrelevant. Core societal functions were deregulated and streamlined in anticipation of a peaceful and liberal new world order.

[1] The Swedish concept of "total defence" includes all activities needed to prepare Sweden for war. Total defence contains both military activities (military defence) and civil activities (civil defence).

The concept of security was broadened and reinterpreted through a postmodern lens: states and their sovereignty were set to reduce in importance. The focus shifted to human security, life, health and welfare. To the extent that threats were foreseen, they were of a new kind and the actors were non-military and non-state, such as climate change, pandemics, large-scale migration flows and terrorism.

Russia's more aggressive stance after 2007 and its war in Georgia in 2008 should have served as a wake-up call, but Sweden and the rest of the West pressed the snooze button. To be fair, more robust objectives focused on state security, sovereignty and freedom of action in the face of external threats did appear in the 2009 defence bill alongside the earlier postmodern "objectives for our security". The armed forces were also asked to "assert Sweden's sovereignty, protect sovereign rights and national interests" and demands for military preparedness increased. Nonetheless, the emphasis on keeping costs down and on peacetime operations eclipsed these signals. As late as January 2014, the then Prime Minister, Fredrik Reinfeldt, declared that an interstate war in Europe was no longer conceivable.

Consequently, it was a brutal awakening when, less than two months later, Russia invaded and annexed Crimea. It suddenly dawned on Sweden that the world had become dangerous again. Russia was rejecting the European security order and trying to carve its own sphere of influence using threats and violence. Moreover, in a conflict between Russia and NATO, the Baltic States would be NATO's Achilles heel. Thus, the Baltic Sea area became the focal point of the new Cold War – and if war should come to the region Sweden would inevitably be drawn in. To make matters worse, in 2016 the United Kingdom voted to leave the European Union and Donald J. Trump was elected President of the USA, which raised doubts about whether NATO and the EU could be counted on as reliable counterweights to Russia.

Despite the heightened tension, the risk of an open war is low. Even though we live in a state of formal peace, however, a struggle for power and influence is under way in the region. Major Russian exercises, threatening fly-pasts and new weapon systems should not be seen primarily as preparations for war, but as a form of "strategic bullying" where the message is that neighbouring countries are small and weak, Russia is big and bad, and the USA had better stay away. This message is reinforced through a skilful campaign of psychological warfare that uses digital media to spread mistrust of Western decision-makers and tries to undermine Western unity. Thus far, however, unity has prevailed and the Russian campaign seems to have had the opposite effect. The countries in the region are now strengthening their armed forces, and the USA and other major Western powers are paying much more attention to the neighbourhood.

Vulnerable Sweden

After Russia's land grab in Crimea, Sweden appeared poorly protected and the postmodern security agenda of the 2000s seemed passé. National security could no longer be taken for granted and we became painfully aware of threats and vulnerabilities that had earlier been ignored. It was not just the weakness of the military defence or the fact that Russia had new weapons – it was also the absence of a civil defence and society's heightened susceptibility to power outages, cyberattacks and other disturbances. The mental map needed to be drastically adjusted, the security agenda rewritten and new priorities set. It is possible to argue that Sweden quickly tumbled down Maslow's hierarchy of needs, from being a global do-gooder to ensuring its own security and survival.

This became apparent from the 2015 defence bill and the process that preceded it. The general public's perception was that defence spending would increase somewhat and Gotland once again be defended by troops, but there were also other important signals, for example the return of concepts such as national defence, state sovereignty, war-fighting capability and mobilisation. Furthermore, operational capability was re-emphasised, conscription reinstated and a new version of total defence planned. Attention to the needs of war and preparedness were again to be made part of public planning.

Early in 2017, the government presented its *National Security Strategy*, developed by the Cabinet Office, in which Sweden's national interests are articulated. As a strategy, and as a policy document for the administrative authorities, the document falls short, since it is something of a wish list without clear priorities or any indication of how the objectives are to be met. Nonetheless, the strategy is the first official and public expression of Sweden's national interests.

Sweden's national interests

Sweden's political class has a long-held disdain for the notion of national interests, since the term is derived from the Realist school of international relations – a coldly calculating tradition that emphasizes self-interest and rejects idealism. Thus, the concept was anathema to the foreign policy establishment in the decades when Swedish foreign policy was shaped by progressive values and aimed to play a global role. Nonetheless, actual policy continued to be governed by national interests, as has been the case since the early 1800s.

It is the national interest not to end up in a war with Russia that has been behind the policy of careful neutrality pursued since 1812. Similarly, it was the national interest in having a counterbalance to Russian influence that was behind our discreet – and at times secretive – reinsurance policy towards the Western powers. Our national interest also guided the departures from a line of strict neutrality that kept us out of the Second World War. In addition, when the Swedish model of the mixed economy crashed in 1990 it was the need for a functioning economy that suddenly turned EU membership into a national interest.

Using national interests as an analytical tool and a guide to practical policies makes it possible to shed light on structures and circumstances that are often taken for granted, but require attention and care if they are to persist. For example, the current regime of free trade and freedom of navigation is a prerequisite for our national welfare, and our national security is dependent on the existence of barriers to the renationalisation of European security, as well as on the US nuclear weapons-backed security guarantee for Europe.

Although the national interest is a useful concept for analysis and for the pursuit of practical policies, it is problematic in some respects. Its proponents often portray national interests as objective and bordering on the irrefutable. While this may be the case, the national interests exist only at such an elevated level of abstraction that they are also useless as a guide to policy. To guide policy, one must also be able to derive answers from these fundamental interests about *how* these objectives are to be attained, and *with what*. This is where an unavoidable degree of subjectivity enters the picture, not least because there are often several alternative ways to achieve the same goal.

Another problem is where to draw the line between values and interests. In some cases, there seems to be a measure of overlap, since values that are central to a nation's self-image – such as democracy – are also seen as national interests. On other occasions, values and interests clash. This has obviously been the case recently concerning the global ban on nuclear weapons, weapons exports and Swedish policy on the Arab world.

Finally, it must be possible to weigh national interests against one other. For instance, Sweden could further its economic interests by purchasing Russian gas, since it is cheap, but its security interests would be imperilled due to the dependence arising from such a transaction. Competing interests must therefore be ranked or weighed against each other. The outcome of such a priority setting procedure is often context-dependent. When relations are friendly, it may seem unproblematic to say yes to a Russian gas pipeline, but if the situation is tense and threatening priorities will be different.

This phenomenon helps explain the recent change of tune in Sweden's security policies; its sharp criticism of Russia's aggressive acts, ongoing upgrading of its armed forces and increasing emphasis on military cooperation with neighbouring countries, the USA and NATO. These changes have been dubbed the "Hultqvist doctrine", after the defence minister, but are of course also supported by the prime minister.

From wish list to realistic strategy

Despite the important steps taken in recent years to adapt to a more threatening and dangerous world, most notably recent agreement on the 2018–2020 defence budget, the reorientation comes across as fumbling and half-hearted. The government's national security strategy still in large part resembles a wish list. Most of our structures, systems, thought patterns and attitudes are shaped by the decades when no dangers appeared to loom. The outsourcing to foreign companies of sensitive IT services by the Swedish Transport Agency, the city of Karlskrona's installation of a web camera to record the movements of naval vessels and the port of Karlshamn's refusal to decline a Russian gas pipeline are just a few examples of security issues still not being taken seriously. Several chapters in this volume highlight potential threats to national security – but few strategies or tools are in place for coping with these risks.

The government now says that national defence is a core task of the state and claims to be committed to enhancing security. Despite certain increases in spending, however, the military and civilian defence budgets still hover around 1 per cent of GNP. No new capabilities are to be funded and the cash infusion will only suffice to fill the worst shortfalls in funding from the 2015 defence bill – this at a time when it is predicted that the state budget will be in record surplus. If the government is serious and the cause is urgent, shouldn't we expect a little more?

National security is costly and cumbersome, since it makes the execution of tasks more complicated and difficult. In past decades, Sweden knowingly and unknowingly under-financed its armed forces and dismantled the elaborate system of total defence system (see Chapter 2). Worse still, the security implications of our dependence on the electricity grid and on Internet services have not been taken into account. This exposes us to significant vulnerabilities that an aggressor could exploit in times of war or crisis. Today, awareness of the altered threat environment has finally begun to sink in, but the political will to finance reforms and change ingrained habits still lags behind.

An increase in funding and the addition of other resources are urgently needed, but so is a clear shift in Swedish strategic thinking that takes account of the demands that a more precarious world places on Swedish society. To successfully navigate the tense geopolitical situation, it is of vital importance that Sweden's decision-makers have a clear picture of what our national interests are, how – if need be – these can be weighed against one other, and the means and methods essential to achieving them.

Further Reading

Robert Dalsjö, "Hubris, Nemesis and the Search for Kryptonite: Why Eternal Peace Lasted Only 25 Years", blogpost, 19 January 2017, on the *Defence and Security* blog, Royal Swedish Academy of War Sciences, www.kkrva.se.

2. Defence Economics and Defence Allocations: Between Considerations of Need and Cost

Peter Nordlund and Mikael Wiklund

In Sweden, it has long been politically acceptable to take certain defence capability risks for the sake of other policy areas. As the security situation rapidly worsens, this acceptability is diminishing. Earlier political decisions and problems with calculating the level of defence inflation have created an imbalance between military capability requirements and resource distribution. Research shows, for example, that a significant amount of current defence policy is not being managed by political decisions, but is controlled by unintended technical financial limitations about which there is little political awareness. As a result, defence and security policy continue to be affected by a high level of unconscious acceptance of political risk. Reducing this political risk-taking will require financial allocations that better match political ambitions and a revised system for compensating the defence for inflation and cost escalations.

A decrease in defence purchasing power

The purchasing power of the Swedish Armed Forces, or the amount of financial resources and what they can buy, has been decreasing for some time. Purchasing power shrank by approximately SEK 19 billion between 1999 and 2014 on an annual basis. To obtain the same purchasing power in 2014 as it had in 1999, the armed forces' allocation would have needed to be approximately SEK 61 billion, as opposed to SEK 42 billion.

One way to assess defence purchasing power beyond the level of financial resources is to calculate defence allocations as a percentage of GDP. Assessing the percentage of resources that a society spends on defence allows comparison across different countries. GDP levels can be somewhat deceptive, however, since they say nothing about military requirements or military capability. They should therefore not normally be decisive in decisions on allocations. They can, however, be a useful starting point when comparing the distribution of the economic burden among countries cooperating within the European Union or among NATO member states. That way, countries will contribute in proportion to their financial capacity. NATO's recommendation that 2 per cent of its members' GDP should be spent on defence is an example of this. Changes in defence expenditure in absolute terms over time probably provide a clearer picture of the development of military capability than the percentage of GDP allocated to defence. Table 2.1 shows the change in defence expenditure in a selection of regions and countries since 2000.

Table 1. Defence expenditure, 2000–2015. Source: SIPRI. Fixed prices USD.

Region/Country	Defence expenditure % change
World	+ 55 %
Europe	+ 16 %
Nordics (excl. Sweden)	+ 19 %
Russia	+ 216 %
USA	+ 44 %
Sweden	- 14 %

Thus, Sweden's defence spending has declined substantially in both absolute and relative terms, which gives a clear indication that its relative defence capability has been significantly diminished.

There are several reasons for this decline:

First, political positions have changed the objectives of the armed forces and therefore the extent of their activities. These changes have gone hand-in-hand with the reductions in allocations. This can be observed in successive budget bills and the subsequent management of the armed forces.

Second, actual purchasing power has been influenced by technical issues linked to how defence costs increase and how the armed forces are compensated for these increases. The issue is a combination of:

- cost changes in so-called *intermediate goods*, such as personnel, materiel and premises;
- how efficiency and productivity changes are treated in the defence sector; and
- the annual recalculation of allocations to compensate for changes in the price of intermediate goods.

Prices and salaries in the defence sector are recalculated according to its own index – *Försvarsprisindex* (Defence Price Index, DPI). The DPI is made up of different official and non-military indices that are used to compensate the armed forces for inflation. The purpose of the recalculation is to ensure that the activities of the armed forces are governed by political decisions and their financial implications rather than by unpredictable fluctuations in prices, salaries, currencies, interest rates or inflation in other countries.

Problematic recalculations and the demands on defence

Ideally, the DPI should ensure that the defence budget is neither over- or undercompensated for changes in the market prices of the armed forces' intermediate goods.[2] Research shows, however, that the DPI has substantially undercompensated the armed forces for price and salary changes. About half of the erosion in purchasing power between 1999 and 2014 was due to this undercompensation. The unintended financial limitations thus stand for approximately half of the financial policy pursued in the defence area.

Furthermore, technical changes in 2012 to the principles by which the DPI is calculated resulted in a reduction in the annual allocation of approximately SEK 1.3 billion at 2015 prices, or at least SEK 6 billion over the period of the subsequent defence bill. The 2015 defence bill contained a political ambition to add at least SEK 10 billion to defence spending in the period 2016–2020. Because of the technical adjustment to the DPI, however, the real boost will be only SEK 3–4 billion.

In addition, the amount of compensation calculated and the actual economic circumstances of the defence sector have very little in common. In the end, it is the capacity and opportunities for political control that suffer. A basic problem is that the DPI is based on civil official indices. This means that the armed forces' allocations, and with them views on efficiency and productivity, are by and large based on developments in the prices and efficiency of those markets represented in these civilian indexes. In addition, the DPI has a built-in deduction that has to be matched by internal efficiency savings in defence structures – the so-called *productivity deduction.* This, too, is based on a civil construct: productivity developments in the private services sector.

[2] The built-in *productivity deduction,* which aims to create "efficiency pressures" on the defence sector, is an exception (see below).

Even though you can argue that the conditions for productivity are worse in the defence arena, the armed forces are often subject to double productivity and efficiency requirements. This occurs, when politicians' allocation decisions impose new tasks without the corresponding financing and then expect the armed forces to finance the new tasks through rationalisations or efficiency savings. A variation on this theme occurs when the allocation is reduced without reducing the number of tasks, using the same argument about efficiency gains. Politicians do not always grasp that productivity requirements are already embedded in the DPI. The result is that the armed forces end up with two overlapping productivity requirements. The embedded annual productivity requirement has fluctuated between 0.9 and 2 per cent per year, which corresponds to 200–400 full-time and 300–400 reservists to be "rationalized" each year. All this is supposed to be achievable without any effect on defence capability.

There are numerous reasons why the armed forces' cost changes diverge from the civilian assumptions in the recalculation. One important factor is the difficulty of continually rationalizing activities. Other factors include:

- the goods and services in the defence sector are different from those included in index;
- the exposure to various currencies is different from DPI assumptions;
- the markets in which the armed forces obtain intermediate goods are characterized by monopoly and oligopoly;
- activities are characterized by large fixed costs with few opportunities to change materiel systems or personnel, which makes adapting production a slow process;
- the armed forces have to factor in the political climate and political factors, such as regional and industry policies and requests for international cooperation on the procurement of defence equipment, which restricts its freedom of action.

The main differences stem from the fact that the armed forces often use unique resources to produce equally unique products and impacts, which are often difficult to assess. Nonetheless, the consequences of not living up to the requirements of the recalculation can be serious. Shrinking resources force the armed forces to make cutbacks in activity, which eventually reduces their defence impact. This is not the intention of the recalculation.

One example of the differences between the defence market and the civilian market is the cost of defence materiel. Research indicates that rapid cost rises are occurring for defence materiel compared to general inflation. A cautious estimate indicates a growth rate of approximately four per cent above the consumer price index. This means that given the current size of the defence establishment, stocks of defence materiel are going to shrink rapidly if allocations only increase in line with general price inflation. Allocations that are only adjusted in line with general inflation make it impossible to maintain both permanent materiel stocks and the size of the defence organisation.

An underfinanced defence budget?

For many years defence has experienced successive diminutions in capability as a result of reduced financial resources. The 2015 defence bill was a break in this trend, when for the first time in a quarter of a century it called for an increase in defence expenditure and an expansion of purchasing power. The problem is that the starting point for the 2015 bill was the long-term underfinancing of the previous defence bill to the tune of SEK 4 to 6 billion in real terms per year.

There is a substantial risk that the 2015 defence bill has also been underfinanced for achieving the level of political ambition expressed. This is partly due to the "deficit" from the previous defence bill and partly a result of uncertainty about whether the increased ambitions have been completely financed. It is also partly due to the fact that the structural flaws in the DPI recalculation mechanism continue to widen the gap.

In the armed forces budgetary assessment for 2018, the commander-in-chief has highlighted an additional requirement of at least SEK 6 billion in the current (2015–2020) defence bill period. This need is mainly a consequence of unfunded price increases. Some of these are the result of currency effects tied to procurement decisions, such as the JAS 39 Gripen E. The statement can be seen as an indication that as long as the DPI ignores the actual price and costs of armed forces procurement, financial resource allocation will continue to fall behind and never catch up with need. Politicians will therefore have to choose between allocating extra resources to the armed forces or accepting that the armed forces' deliverables will never correspond to political demands. A new Defence Agreement was achieved between the political parties in August 2017. It addresses the deficiencies identified in the armed forces budgetary assessment and provides the funds needed to cover the remainder of the current defence bill period. While this obviously improves the situation in the short term, it does not remedy the deterioration in defence capability caused by long-term underfunding. In addition, the DPI risks blowing new holes in defence spending by continuing to undercompensate for price increases.

Defence resources: a question of risk-taking

Political decision-making on defence-related resources is ultimately about agreeing on the level of acceptable risk. Security allocations, that is, those means that are distributed to defence, must be balanced against the uncertain costs of not being able to manage serious future threats or events. The question then arises: which risks are acceptable in relation to which policy areas and what people are willing to pay? The problem lies in the need to build up military capability before serious events occur, if they are going to be useful in any meaningful way. This means that politicians must divert resources for managing hypothetical *potential* threats and risks, at the expense of *immediate* needs in other policy areas. The temptation to underestimate risks, and thereby free up resources for other things, is obvious. The similarities with home insurance are clear; it is bought because of the risk of fire, but the premium takes resources away from actual and immediate needs.

The political calculation, and thereby the risk of getting it wrong, lies in the question of how great the consequences of a serious event might be to still be acceptable, compared to the amount of resources that a reduction in risk can be allowed to cost.

Ideally, this process of setting priorities and risk levels will be a conscious one that is subordinated to explicit political decision-making. If the purchasing power of defence shrinks, this should be a function of how politicians consider that the risks have decreased or of society being willing to accept greater risks. Research shows, however, that major aspects of actual decision-making are handed over to automatic technical mechanisms to recalculate allocations. In other words, major parts of political risk-taking lie beyond direct political or parliamentary control. When there is also a systematic tendency to undercompensate for actual increases in prices and costs in the defence sector, the result is that risk-taking exceeds stated political intentions. In addition to raising allocation levels, it should therefore be of the utmost importance to examine the construction of the price and salary compensation in the DPI, with the aim of making it more consistent with actual price, cost and salary changes.

Inadequate defence capabilities mean that politicians must expect risks to manifest themselves to a greater extent in unwanted events, while at the same time such events will become more serious. Even if it is difficult to put a price tag on this, it must still be considered a price – in the worst case an existential one – that over time will have to be paid. The costs of managing a defence-related risk arise in terms of kronor and the state's budget. The costs of ignoring such a risk are incurred in the form of reduced political room for manoeuvre, a decrease in the influence of democratic freedoms and rights, a weaker international system, threats to the nation's existence, and shortcomings that affect the lives and health of citizens. If the costs of risk management fall short of the costs of leaving risks unaddressed, it is socio-economically rational to redistribute resources to an increase in defence capability.

Ultimately, the choice, in terms of defence finances, is about finding a way for the political demands for capabilities to keep in step with the allocation of financial resources. Historically, there has been a tendency for resources to fall behind compared with political ambition concerning defence capability. The time lag between ambition and money has traditionally been one defence bill period of five years. This time, too, it is evident that an increase in allocations is needed to match political ambitions. Perhaps new allocations will be needed during this defence bill period, even though the recently added allocations have improved the economic situation of the armed forces. More than anything, a substantial increase in defence spending is needed for the defence bill period 2021–26. Otherwise, it is unlikely that politicians will be given the defence capabilities they expect, with the associated costs this entails in terms of increased security risks.

3. The Baltic Sea Area: a New Geopolitical Focal Point

Mike Winnerstig

The Baltic Sea area currently finds itself in geopolitical focus. The Baltic countries are small and difficult to defend, and even a limited attack against them would mean that Russia would be able to challenge both NATO and US leadership globally. The probability of this is low, however, since the risks for Russia are high and have become even higher since the spring of 2017, when NATO began to position military units in the Baltic countries and Poland. These forces are comprised of just one battalion-sized battle group per country, but constitute an effective "tripwire" against Russian conduct. In the event of any military conflict in the Baltic Sea area, however, Sweden's territory will be engaged. It is therefore vital that Swedish decision-makers understand the region's geopolitical dynamics.

The Baltic Sea area in strategic focus

Sweden's neighbours, especially the Baltic Sea countries, have come into military-strategic focus in recent years. This situation is different from the Cold War, when the focal point was the central front, in the middle of now unified Germany. From the Swedish perspective, the Baltic Sea area was not without drama during that time, but geopolitically it was something of a backwater. Today, however, the Baltic Sea area is a focal point for the growing confrontation between Russia and the West.

Russia's aggression against Georgia in 2008 and in Ukraine since 2014, while in themselves nothing to do with the Baltic Sea area, demonstrated Russia's willingness to use military force for political purposes and served as wake-up calls for all the smaller countries in Russia's vicinity, including Sweden and Finland. This is in addition to the type of information warfare that Russian has long pursued, especially against the Baltic states. Within the latter framework, with the aim of destabilization, Russian actors have disseminated the message, among other things, that the Baltic countries have no credibility as states, their political establishments are engaged in persecuting their Russian-speaking minorities, and that they have a "fascist" past that is reflected in their current politics. This type of "active measure" contributes to the image of a Russian revanchism in the region, which, along with the significant Russian rearmament process over the past ten years, awakens apprehension over future Russian military action.

Sweden's central position in the Baltic Sea area means that any security developments in the region are also going to be decisive for Swedish security. Understanding how geopolitical dynamics function in our neighbourhood should thus be of vital importance to Swedish decision-makers.

Focal point Baltic

The Baltic states are small in both territory and population; they lack strategic depth and have limited armed forces and no air force. If Russia's geopolitical revanchism were to express itself again in the future, this makes them the most exposed of the NATO countries. Were Russia seriously willing to challenge the West and US global leadership militarily, this would most easily be achieved by a limited attack against some part of a Baltic country.

Such an action would present the USA and other NATO members with the choice of either actively beginning a war against Russia – which could theoretically quickly shift into some form of nuclear war – or meeting Russia halfway through some form of negotiated solution. The latter alternative would effectively undermine US leadership in the eyes of the entire world and probably also lead to the dissolution of NATO, since the organization would have failed in its prime mission – to defend the territory of a member country. In many Western capitals, none of these alternatives are appetizing.

However, the overall picture is not so bleak as it might initially appear. The probability of Russia being willing, without provocation, to risk war against the entire Western world is not especially high. The military geography, moreover, is relatively favourable for the Baltic states. Much of the region bordering Russia and Belarus consists of lakes, marshes and similar terrain that would be relatively easy to defend if army units were in the area. In addition, the Baltic countries have made large defence commitments in recent years: Estonia has long spent 2 per cent, or somewhat more, of GNP on defence; and both Latvia and Lithuania will reach this level in 2018. Estonia and Lithuania are currently planning for two brigades of ground forces each, which is the same level that the Swedish armed forces aim for. The fact remains, however, that none of the Baltic states could manage to defend themselves for long on their own against a Russian opponent. Resolving their defence problem through integration with both the EU and NATO has therefore been an obvious solution for the Baltic countries ever since they regained their independence more than 25 years ago.

The US and the defence of the Baltic Sea area

From a Baltic Sea perspective, the USA is the only Western power capable of seriously balancing Russian military revanchism. This state of affairs has not always been clear in Washington, DC. Every US president since the end of the Cold War has begun his term with a positive attitude to Russia and by declaring a willingness to create a better relationship with that country. An especially clear example was Barack Obama, who initiated the so-called reset policy towards Russia in 2009, even though only a year before the Russian military had occupied large portions of the territory of a loyal US partner country, Georgia. As late as 2012, Obama took the decision to halve the number of US army brigades permanently stationed in Europe, and to withdraw all the USA's heavy tanks from the continent. Russian actions in recent years – especially regarding Ukraine in 2014 – once again made Russia a strategic enemy of the USA in the eyes of the Obama administration. That the 2017 Trump administration, especially President Donald J. Trump himself, has an explicit agenda to improve relations with Russia is, in this light, just a variation on an earlier theme.

Trump's political ambition has, however, already been outflanked by military realities. The US Department of Defense continues to implement the plans decided on by the Obama administration to strengthen the defence of the most exposed European allies. Within the frame of the *European Reassurance Initiative* (ERI), obvious military pre-positioning of US troops and material is now under way. The aim is not just to reassure the European NATO member states of US support, but also to actively deter Russia from acting militarily against any NATO country. The US European Command (EUCOM) has regained its heavy units, including tanks, which train jointly and build the capability of the Baltic countries as well as Poland. EUCOM has also regained its status as a "warfighting" command, having been in a largely supporting role since the end of the Cold War.

During Obama's final four years, the commitment to ERI was quadrupled in monetary terms. In the Trump administration's first budget, for 2018, a further 40 per cent increase is proposed. It is therefore possible to claim that even if the president's rhetoric is noticeably Russia-friendly, the Pentagon's resources go where the geopolitical problems are. For Europe's part, this means the Baltic Sea area.

There are several reasons for this. The most obvious is that a successful Russian challenge to NATO – and the NATO Treaty's article 5 on collective defence – would powerfully undermine

US global leadership. The second is that central actors in the Trump administration – such as the Secretary of Defense, James Mattis, the Secretary of State, Rex Tillerson, and the National Security Adviser, H.R. McMaster – are not naive about Russia, but perform realistic geopolitical analyses of the country's actions and the US countermoves that are required.

President Trump's own position in this matter is, at time of writing, unclear. He has expressed considerable understanding of Russia, and especially for its president, Vladimir Putin. At the same time, he has strongly criticized European NATO member states for their inadequate commitment to their armed forces. He has not, on the other hand, reduced the US military commitment to Europe and the defence of small European states against potential Russian aggression. On the contrary, as mentioned above, he proposes to increase substantially the US budget allocation for this purpose. It is possible to interpret his criticism of European NATO members as a negotiating tactic, whereby Trump, through his criticism and relative unwillingness to express unconditional support for NATO, seeks to force the European members to increase their defence expenditure. Most NATO countries today clearly spend less than the 2 per cent of GNP that the organization defined as a minimum when Obama was president. Trump's rhetoric and criticism should thus perhaps be seen less as a part of his view on Russia and more as a new US strategy to increase European defence commitments, which in many cases are directed precisely at meeting possible Russian aggression.

NATO and the Enhanced Forward Presence

In contrast to the situation during the Cold War, a majority of the Baltic coastal states are now NATO members and consequently participate in the organization's joint defence planning. For a long time after the official inclusion of the Baltic countries as NATO members in 2004, NATO's military structure did not carry out any defence planning for these countries. It was not until 2010 that NATO as a whole began to take the Baltic Sea area seriously from a military-strategic perspective. The existing defence plans for Poland – which Poland had demanded when it became a member of NATO in 1999 – was broadened to include the Baltic states. This was controversial at the time, since several influential NATO countries opposed such planning, which would portray Russia as the only imaginable enemy – something which Germany and some NATO officials considered unnecessarily provocative.

After Russia's aggression against Ukraine and the annexation of Crimea in 2014, it became simpler to argue that there was a need not only for defence plans, but also for substantial defence resources for the new so-called front states, primarily the Baltic countries and Poland. The NATO Summit in Warsaw in 2016 established a new concept: an *enhanced Forward Presence* (eFP). This comprises NATO units that are based for longer periods in the front states. Through their presence and their battle capability, they constitute an essential contribution to the defence of these countries. The concept was operationalised as one battalion-sized battle group per country plus support units from additional NATO countries. It was also decided to implement this relatively quickly, beginning in early 2017.

During the summer of 2017, the concept was put into effect in all the front states. A British heavy infantry battalion has been based in Estonia, along with a French mechanized infantry company. In Latvia, there is now a Canadian motorized infantry battalion, a Spanish mechanized infantry company and a Polish battle tank company, together with lesser support units from Italy, Slovenia and Albania. In Lithuania, Germany has based a mechanized infantry battalion, which is supported by a Norwegian infantry company and units from the army of the Netherlands, among others. In Poland, the USA has based a battalion-sized battle group from the motorized brigade that the USA has permanently stationed in Germany. In addition, the UK and Romania have also contributed modern battle units within the Polish part of eFP.

At least 12 NATO countries now participate in the direct defence of the Baltic countries and Poland. The troop strength is slightly more than 1100 soldiers per country, which means that the entire operation is about the size of a brigade, or around 4500 personnel. From a military standpoint, this is of course primarily a so-called tripwire unit. This means that on its own the force is not large enough to be able to deter a military attack from a major power such as Russia but in the event of such an attack, the aggressor would enter directly into war with half of NATO at the same time and indirectly with the entire Western world. The deterrent effect should be considered very large. That the force is no greater than one battalion-sized battle group per country also means that it cannot be claimed that it is capable of offensive military action: It is much too small for that. Given the military-geographic realities and the growth of the Baltic armed forces, these forces could – after the requisite joint training – also directly contribute in a substantial way to the defence of the Baltic countries.

Depending on the degree of early warning and the amount of resources an attacker commits, the Baltic and Polish armed forces – together with NATO units – could serve as an effective brake against a substantial Russian military attack. Additional resources would include NATO's established rapid response forces, such as the NATO Response Force (NRF) and the Very High Readiness Joint Task Force (VJTF). The NRF (maximum 40,000 soldiers) and VJTF (about 5000 soldiers) have no permanent base, but are deployed according to need.

Through these measures, NATO may have found a reasonable balance between deterrence and provocation. Russian representatives and the Russian media depict the entire process as destabilizing for the region, perhaps because it ought to reduce Russia's discretion or freedom of military action in the region.

Consequences for Sweden

Over the past two decades, and with relatively broad political unity, Sweden has replaced its traditional neutrality policy with a solidarity policy, as it is called in the report of the Parliamentary Commission on Defence Policy (*Försvarsberedningen*). Sweden is not a member of any military alliance but it does have obligations – of a type that are still not clearly defined – to all EU member states by virtue of the Treaty of Lisbon (article 42:7). In addition, since 2009 it has made declarations of solidarity with all the EU member states and the Nordic countries. Every imaginable military conflict in the Baltic Sea area would lead to Sweden's territory being much coveted by the warring parties, especially for operations directed at the Baltics.

This means that Sweden is likely to be rapidly drawn into a conflict process. The security situation in the Baltic Sea area today has more similarities with the Cold War than at any time since 1991, albeit that it lacks any strong ideological dimension. Geopolitically and militarily/strategically, however, the focal point of the conflict has moved considerably closer to Sweden. This is something that Swedish decision-makers and the Swedish defence establishment are now being forced to deal with. Good insights into the geopolitical dynamics of the neighbourhood are a necessary foundation for this.

Further Reading

Mike Winnerstig (ed.), *Tools of Destablization: Russian Soft Power and Non-military Influence in the Baltic States*, 2014, FOI-R--3990--SE.

4. Germany: a New Swedish Ally in Europe?

Eva Hagström Frisell and Anna Sundberg

Germany's importance to Sweden and the security of Sweden's neighbourhood have increased in recent years. Germany and Sweden have also shown an interest in deeper bilateral defence cooperation. At first glance, the prospects for closer defence ties are promising. An analysis of the security policy documents that the two countries have recently adopted, however, reveals that they have fundamentally different views of how national security can best be advanced. Germany and Sweden also have different roles in Europe. While Germany is a centrally located major power that plays a prominent role in European security policy, Sweden is a medium-sized state with more of a regional focus on security and stability.

New preconditions for cooperation

The deteriorating security situation in Europe's neighbourhood and the current challenges to European unity mean that both Germany and Sweden find themselves in the hunt for new cooperation partners. Germany has long been Europe's economic superpower, but has in recent years also emerged as one of the leaders of Europe's security policy. There are numerous challenges to European security to deal with. The expectations of German leadership from the rest of Europe have grown not only since the Russian aggression against Ukraine, but also since the election of President Donald J. Trump in the United States and the United Kingdom's decision to leave the European Union. Europe's traditional major powers in matters of security and defence are much preoccupied with other challenges: the UK must try to find a role outside the EU while struggling to maintain internal unity; and France is primarily focused on dealing with terrorism, both domestic and international.

In recent years, the German government has demonstrated an increased willingness to meet external expectations. Germany's readiness to assume greater responsibility for international security is a recurring message in policy statements and is also reflected in its actions. One example is that Germany has taken the lead in the battalion-sized battlegroup established within the framework of NATO's enhanced forward presence in Lithuania. From a German perspective, however, this is more about assuming responsibility within certain limits. Germany's engagement must not be perceived as overly dominant. Thus, German security and defence policy will continue to be formulated in close cooperation with others, and NATO and EU cooperation to comprise its main pillars.

Sweden also has a strong interest in contributing to stability and security, especially in its neighbourhood, and national defence has come back into the limelight in recent years. In contrast to German decision-makers, however, the Swedish government continues to see military non-alignment as an important principle and exclude both NATO membership and deeper defence cooperation within the EU. Sweden is focused instead on strengthening its bilateral ties with other states. The relationship with the US has a special status. In addition, Sweden has placed extra emphasis on developing its operational military cooperation with Finland. Sweden's declaration of solidarity also encompasses all the EU member states, as well as the Nordic countries. Of the above, Sweden's foremost ambition is to expand cooperation with the other Nordic and Baltic countries. Bilateral cooperation agreements with the UK and Poland have also been signed.

Like Germany, Sweden is influenced by the changes in the security policy landscape. Sweden must find a replacement for the UK as a close partner in the EU and might eventually need another security policy ally than the US. Germany, the major political and economic power in Europe, lies close at hand. The Swedish government has also stated that Germany is playing a key role in stabilizing Sweden's neighbourhood, and thus that it sees a direct connection between German and Swedish security. Sweden and Germany entered a discussion on deepened cooperation in 2016 and the defence ministers of both countries signed a joint letter of intent on cooperation in June 2017. From a security policy perspective, however, defence cooperation with Germany cannot have the same weight as the relationship with the US and the UK, the two major military powers that have the greatest capacity to act militarily in Sweden's neighbourhood.

Recently defined national interests

Germany and Sweden have recently defined their respective national interests. Germany published a new White Paper on German security policy and the future direction of its armed forces in July 2016. The Swedish government released a national security strategy in January 2017.[3] Defining national interests in this way had earlier been politically sensitive in both countries, and there has been an unwillingness to take a stand on these issues.

Even if the documents differ in character and scope, they provide clues about the potential for deeper bilateral cooperation. Both documents have been adopted by their respective national governments, which accords them greater weight and relevance than if they were just the products of their respective defence ministries. That Germany's three largest parties stand behind the document further increases the likelihood that this direction will be maintained over time. The German White Paper was drafted in an inclusive process that offered various parts of society an opportunity to contribute. The aim was to foster a participatory approach, explain German security policy and enrich the debate.

In Sweden, the process of seeking consensus among the political parties on security and defence policy normally proceeds within the framework of the parliamentary commission on defence. Sweden's national security strategy, however, was produced by the government without any direct negotiation with the opposition parties. Prime Minister Stefan Löfven has nonetheless expressed the hope that the national unity that usually prevails in matters of Swedish security policy will also apply to the implementation of the new strategy. The ministers and deputy ministers on the newly established security policy council are to have special responsibility for monitoring the implementation of the strategy.

Consensus on threats and security

The direction of national security policy has thus been set in different ways, but the documents have many similarities. Germany and Sweden both present broad views of security. This is reflected not only in how national security is seen as a concern of the whole of society, but also in how the security challenges identified span a broad spectrum.

Germany and Sweden also share many geostrategic features and these similarities are reflected in their respective threat perceptions. Both documents paint similar pictures of security policy developments in Europe. They describe a worsened

[3] Die Bundesregierung, *Weissbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr* (the document is also available in English: *White Paper 2016 On German Security Policy and the Future of the Bundeswehr*); and Regeringskansliet [The Government Offices], Statsrådsberedningen [The Prime Minister's Office], *Nationell säkerhetsstrategi* [National Security Strategy], January 2017.

security situation, in which Russia is challenging the prevailing security order, while Europe faces significant internal challenges and its southern neighbourhood is characterized by conflict.
The security challenges identified are also to a great extent the same for both countries, even if in practice there are differences in their national security policy debates. Germany, for example, has for many years had a greater focus on terrorism, but this has now also become a central question in Sweden. The national debate in Sweden is focused on the Russian threat in its vicinity to a greater extent than it is in Germany. Both documents, however, present a broad list of challenges and threats, which range from military incidents, disinformation campaigns, cyberattacks and terrorism, to organised crime, climate change and pandemics. In addition, both countries emphasise the importance of a strong transatlantic link and US significance for European security, at the same time as they express support for stronger European integration.

A direct comparison of the national interests listed in the respective documents shows that they are much the same in both (see table 4.1). They differ, however, on two essential points. First, the German White Paper states that a strong German economy and free world trade are in its own security interest, while corresponding statements in the Swedish strategy discuss the promotion of a regulated, multilateral world order. Second, German security interests also include the protection of allies and strong transatlantic cooperation. The Swedish strategy instead considers the promotion of stability and security in its immediate neighbourhood to be in its national interest.

Table 2. Comparison of German and Swedish security interests

Germany's security interests	Sweden's national interests
• To protect the population, sovereignty and Germany's territorial integrity • To protect the population, sovereignty and territorial integrity of allies • To maintain a rules-based international order • To ensure the prosperity of the population through a strong German economy and free world trade • To promote responsible use of limited goods and scarce resources • To deepen European integration • To consolidate the transatlantic partnership	• To ensure the safety, security and health of Sweden's inhabitants • To secure the supply of and protect critical societal functions • To uphold fundamental values: democracy, the rule of law, human rights and freedoms • To defend, under all circumstances, Sweden's freedom, security and right to self-determination • To promote the stability and security of our neighbouring areas • To maintain and strengthen cooperation, stability and integration within the EU • To promote a rules-based multilateral world order

Crucial differences between cooperation priorities

Consensus around threats and challenges as well as the need for a holistic approach to tackling these challenges would seem to be a good basis for deepening bilateral cooperation between Sweden and Germany. After detailed analysis, however, obvious differences emerge. The major difference lies in the priority given to the various forms of security and defence policy cooperation: NATO and the EU have the highest priority for Germany while Sweden instead emphasizes bilateral defence cooperation.

Germany's security is closely linked to its allies in NATO and the white paper highlights the defence of the territories of the NATO members as a central security interest. In addition, NATO is the most important framework for many German bilateral initiatives. By taking the lead as a Framework Nation, Germany is seeking closer relations with other nations that bilaterally integrate forces or capabilities in its armed forces. Germany, moreover, is pressing for deeper EU cooperation on security and defence policy, and sees the EU becoming a security and defence union as a long-term goal. Germany has expressed its support for the creation, together with a core group of countries, of so-called Permanent Structured Cooperation (PESCO) in the defence sector, with the intention of creating a new foundation for initiatives and cooperation projects that promote capability development in the EU member states.

The Swedish government has emphasized that joining NATO is not an option. The defence minister, Peter Hultqvist, has been clear that an application for membership would have far-reaching consequences for domestic policy, neighbouring Finland and stability in the region. At the same time, Sweden's partnership with NATO has gradually developed, and in 2016 parliament ratified a so-called Host Nation Support agreement, which regulates how NATO members can operate on Swedish territory. Sweden has also expressed doubts about a number of initiatives proposed by Germany in order to strengthen European defence cooperation. The Swedish government currently appears to view the EU as a forum for foreign and security policy cooperation and to a lesser extent as a defence policy tool.

Opportunities for deeper cooperation

A comparison of Germany's and Sweden's new policy documents provides few concrete details on possible areas of cooperation. At the general level, the largely broad language indicates a consensus regarding threats and security. Nonetheless, while these types of documents seldom play a positioning role, they do highlight crucial differences in how the two countries ascribe priority to security policy cooperation.

While the Swedish national security strategy identifies Germany as a vital partner, the German white paper lacks any such description of Sweden. This does not mean, however, that Germany is opposed to bilateral cooperation. In recent years, Germany has initiated military cooperation with a range of states in Europe, such as the Netherlands, Poland, Norway, the Czech Republic and Romania. From a Swedish perspective, however, the fact that this cooperation primarily occurs in a multilateral context, and mainly within NATO, might be problematic. For Germany, this is an important arena for legitimizing its role as a major power, but is also useful for securing access to a variety of capabilities.

Sweden and Germany share several flaws in military capability. Both countries have been reducing their defence spending for some time and the proposed increases are far from sufficient to remedy the flaws by themselves. Their armed forces lack personnel and materiel. Their units have a low level of readiness and conduct too few exercises. These capability gaps could form a viable basis for cooperation, which could involve operational cooperation in the Baltic Sea or in international missions, and even joint capability development in terms of materiel and exercises.

The prospects for closer cooperation between Germany and Sweden are dependent on developments in Europe and the rest of the world. Several factors – chief among them the result of the "Brexit" negotiations, the evolution of President Trump's policies, continued Russian actions and the course of events in Europe's southern neighbourhood – could create a new dynamic in European security and defence cooperation. This could develop in several different directions, for example, from closer cooperation between a limited group of countries, to reinforced bilateral relations or deeper European integration. It is not certain, however, that Sweden and Germany will draw the same conclusions about which form of cooperation best favours their national security.

Further Reading

Johan Ellend, Anna Sundberg and Niklas H. Rossbach, *The Russian Wake-up Call to Europe: French, German and British Security Priorities*, 2016, FOI-R--4270--SE.

5. Total Defence at the Crossroads

Fredrik Lindgren and Ann Ödlund

Building a modern Swedish system of total defence must focus on creating maximum defence impact. An important question will be which critical defence activities should be undertaken by the armed forces and which should be delivered by civil defence. The current organisation of governmental organisations, and the division of responsibilities and roles may need to be revisited to ensure the best possible defence impact. Ultimately, the civilian aspects of total defence need to produce a visionary, long-term plan for its active capability development, instead of, as in today's crisis management, allowing its development to be mainly reactive.

Swedish thinking about war and preparing for an armed attack have long been seen as unnecessary and all too expensive. Planning in several areas of society, including crisis management, has not anticipated being threatened by an aggressor, but instead concentrated on handling peacetime events in the form of minor disturbances and short-term supply disruptions. In response to the deteriorating global situation, however, the defence policy bill of 2015 focused on heightened alert and war, and prioritised enhancing the operational capability of battle units as well as planning a cohesive "total defence".[4]

This chapter focuses on the new modern total defence and outlines a number of important points of departure and choices facing its development. The aim is to show how individual questions can influence the cumulative capability of total defence and to contribute some ideas on altering its aims and circumstances.

Towards a modern total defence

Total defence is being rebuilt in order to deliver maximum defence impact. These efforts must examine, among other things, which of the critical defence activities should be taken on by the armed forces; what civilian actors, i.e. civil defence

[4] The Swedish concept of "total defence" includes all activities needed to prepare Sweden for war. Total defence contain military activities (military defence) and civil activities (civil defence). During a state of highest alert (e.g. a state of Sweden being at war or in danger of war) total defence consists of all societies' activities. Swedish law 1992:1403 on Total defence and High Alert/Totalförsvar och höjd beredskap

entities, should be responsible for; and how total defence should be organised to achieve the best possible defence impact. It is questionable whether the development approach that dominates crisis management today, which is mainly event-steered and reactive, is suitable now that society is building its defence capability to the level of heightened alert and a possible war footing. The systems, structures and capabilities put in place now will steer the later development of total defence for a long time to come. It is therefore essential to analyse what readiness levels the various requirements should be set at, and how Sweden's defence should be developed to achieve the best possible defence impact.

The 2015 *Strategic Outlook* highlighted three challenges for the development of civil defence:

- how to manage the so-called grey zone and the transition from the peacetime organization of society to a war footing;
- how to integrate civil defence with current systems for emergency preparedness; and
- how to balance the different goals of civil defence in order to avoid a one-sided focus on the goal of supporting the armed forces.

These challenges remain valid and are also relevant for total defence. Based on what has happened since, however, it is now possible to identify new choices and challenges for the reconstruction of a modern total defence.

At the political level, there is broad agreement about the direction of defence policy and the government's increased economic resources for defence. The response to the government's decision to revive total defence-planning demonstrates a willingness among the authorities and other actors to participate. The attitude to total defence is changing as knowledge and awareness are increased, not least as a result of education and training activities.

In its opinion survey, *Opinioner 2016* (Opinions 2016), the Swedish Civil Contingencies Agency (MSB) found a relatively strong increase between 2013 and 2014 in the proportion of Sweden's population that believed Sweden needed a military defence – a change that has persisted in more recent surveys. In addition, according to the survey, a major part (78%) of the population believed that today's preparedness for dealing with and facing a military attack was inadequate. According to a 2016 opinion poll commissioned by daily newspaper *Dagens Nyheter* and carried out by IPSOS, a majority of Swedes agreed that defence allocations should increase. All the above provides a good basis for building a modern total defence.

Total defence as a concept is focused on antagonist threats, and thus has additional requirements to crisis management. It is therefore not surprising that the return to total defence planning was initially met with some scepticism by the authorities concerned. In a study of wartime organisation and resource increases conducted by FOI in 2014, the governmental agencies with special responsibility for national defence readiness raised the lack of knowledge and resources that hampered their engagement in total defence issues. A clear expression of political will combined with the communication of positive attitudes and signals from their respective leaderships and other decision-makers will be of vital importance to the development of total defence, and not least to changing the mindset that excludes the possibility that Sweden could ever be threatened with war.

Defence impact in focus

Even if planning for total defence has already resumed, the construction of a modern total defence remains a major undertaking. This work must be based on the capability requirements of total defence and the focus must be on collective defence impact, that is, Sweden's capacity to defend itself from attack.

Adopting measures that only improve the capability of parts of the military or of civil defence in isolation is too low an ambition. The measures taken and the special efforts made must all be appraised in the light of a comprehensive assessment of the various aspects of total defence. For example, building a capability to provide long-term support to another actor's activities would be a poor use of resources if that actor's activities are planned to have an expected lifetime of only two weeks.

Limited resources and major development requirements mean that building the capability of different actors needs to be balanced and prioritised, but all the time with the defence impact in focus. Centralised governance using carrots and sticks will be required, but attention must also be paid to the development and adaptation that naturally occur when civilian and military, and private and public sector actors meet, plan and conduct exercises together. In the first case, there must be agreement at the political level to provide central authorities with the prerequisites needed to carry out planning. In the second case, it is the primary responsibility of regional and local authorities to develop efficient solutions based on their specific needs and opportunities. At the extreme, however, both cases involve the identification of areas that are important from a total defence viewpoint, and getting agreement on how resources will be distributed within total defence during a real event, and by whom.

There is also a danger of getting stuck in today's structures, accountabilities and regulations when proposals or initiatives are being presented and assessed. These regulations may need to be changed if the defence impact is to remain the focus, to create the conditions that total defence needs in order to deal with the range of threats that Sweden could face. Since the establishment of total defence in the 1940s – and its subsequent dismantlement at the end of the 1990s – Swedish society has undergone major changes. This is no less applicable to the issue of the market reforms applied to a broad range of societally critical functions where public actors had previously had a dominant role as owners and operators. Therefore, modern total defence must not only be able to deliver new capabilities that meet the needs of today and tomorrow, but also be designed on the basis of different societal conditions.

Total defence at the crossroads

The decisions made today will influence and steer tomorrow's total defence capabilities. There are several fundamentally important questions where choices must be made.

- Which critical defence functions should be carried out by the armed forces and what should be delivered through civil defence?

The division of responsibility between civil and military defence is not clear. When responsibilities are being assigned and resources distributed, a central question should be: which tasks are best performed under the auspices of the armed forces and which should be assigned to civil actors? Examples of where such choices need to be made include health care and the supply of food, fuel or other necessities to units of the armed forces. Different alternatives should be considered and weighed against each other but the focus should be on the best possible defence impact even if this means that other interests have to take a back seat. The combatant status of civilian actors is a vital question that includes protection levels and security for the personnel categories and distributors concerned.

Planning for total defence and other preparations will result in the identification of a range of specific civil and military requirements connected to heightened alert, and the solutions chosen to meet these requirements must be based on today's deregulated society and leaner armed forces. The search by public and private sector actors for cost-effective solutions means that many critical societal functions have little or no redundancy built in for anything other than minor disturbances. This is sufficient for peacetime events, which can be dealt with through redistribution, but such capabilities are likely to be inadequate in the event of an attack on Sweden. We do not believe, however, that it will be possible to accumulate sufficient redundancy for society to function normally during a war situation. From a total defence perspective, different functions are not equal in importance and some capabilities must be prioritised over others. There are also differences in the requirements that will be placed on different municipalities and counties, depending on their geographic and military-strategic location.

- How should total defence be organised for the best possible defence impact?

Sweden's official defence organisation is based on sectoral divisions, for which different authorities have designated areas of responsibility, and geographical divisions at the central, regional and local levels. Its focus on the national territory probably means that the geographic dimension needs to be more prominent and clearer in the organisation of society's total defence capability. One problem that affects both total defence and crisis management is the fact that the geographical boundaries of government agencies at the regional level are inconsistent. This complicates collaboration. A unified higher regional level that comprises several counties would simplify coordination of total defence and also of crisis management. A uniform geographical division of state activities at the regional level would simplify coordination.

There are several ways to organise at the higher regional level. A county administrative board might for example be given extra responsibility and resources for a larger area that corresponds to the military regions of the armed forces. The MSB could organise some of its activities in a way that strengthens their geographic dimension, with the aim – within the framework of its responsibilities for civil defence[5] – of providing better and more targeted support to actors at the regional level, most notably the county administrative boards. There are two possible ways to achieve this. The less sweeping one would be for the MSB to organise units that primarily support the county administrative boards and municipalities in their work. The slightly more extensive one would be for the MSB to establish a regional presence that mirrors the higher regional level. In addition to supporting the higher regional level, a regional presence would improve the MSB's ability to represent the needs of civil defence to the central government.

The new special responsibility for readiness only affects certain central authorities. Other equally important authorities are absent from current planning arrangements. The six existing cooperation areas that form the basis for coordination are also poorly suited to concrete planning, since they encompass so many different activities. These should be replaced by clear sector responsibilities, where one authority in each respective sector has responsibility for coordination in order to facilitate unified planning and capability development.

The overall principles on coordinating and prioritising society's resources need to be further elaborated – not just the capabilities of individual actors. Central and regional directories of critical resources would facilitate an overview of what is available, which would in turn make it easier to make decisions about the distribution of these resources. An examination is also needed of what stocks of important supplies are needed, which contracts need to be signed or revisited and the measures required to prepare for requisitioning (according to the law on requisitions) for the needs of total defence.

- Will crisis management's event-driven development work for civil defence?

The evolution of peacetime crisis management – and with it the foundation of civil defence – has in recent decades been primarily event-driven and reactive. Experience and analyses of serious events and the management of major crises have formed the basis of measures to enhance the capability to manage future crises.

[5] According to its administrative instruction, the MSB should: "represent civil defence at the central level on questions of significance to deliberations on civilian and military need for societal resources, in the absence of specific regulations"

In the revived planning for total defence, it will be necessary to proceed from plausible assumptions about the possible concrete acts of war that might strike society, rather than from experience of previous crises. Certain long-term analyses are already being conducted in the area of crisis management. There is therefore no lack of supporting material on the future development of various capabilities, but this also needs to be weighed against the requirements of total defence. If civil defence is to avoid being imbued with the same kind of event-driven ethos as crisis management, strategic decision-support materials must be produced, including alternatives for maintaining and developing civil defence, that have the impact on defence in clear focus. The so-called *perspective* studies performed by the armed forces are an example of how a cohesive forward-looking analysis can be translated into an analysis of future capability needs.

Increased engagement and new opportunities

Who will do what in situations of heightened alert – civilians or the militarily, the private or public sector – is a fork in the road where the greatest challenge is likely to be to reaching agreement on long-term solutions at the political level, which can then be confirmed by the central authorities. The core principles for organising total defence is another area where several alternatives should be analysed, as well as the issue of whether – and if so, how – civil defence should develop a long-term planning process.

Thus far, the renewed focus on total defence planning has primarily involved the armed forces, the MSB and the other governmental agencies with special responsibilities linked to situations of heightened alert. More agencies need to be engaged in this development work; these include the defence agencies (e.g. the Swedish Defence Materiel Administration, FMV, the National Defence Radio Establishment, FRA and the Swedish Defence Research Agency, FOI), other central authorities, the municipalities and county councils/regions, as well as industry and business. Furthermore, sector-wise analyses and assessments, as well as consideration of geographical conditions and differences, will be central to achieving functioning and credible total defence planning.

Interest in and awareness of total defence have increased in recent years. Today’s more explicit political priorities, along with broader societal engagement, create a window of opportunity for changes to and the development of total defence that should be exploited. This chapter has highlighted several important choices regarding the continued development of total defence. A focus on the collective defence impact may seem obvious, but different interests, forces and agendas – as much civilian as military – risk obscuring the overall aim – to construct a total defence that is capable of facing an armed attack against Sweden.

6. Psychological Defence: Vital for Sweden's Defence Capability

Niklas H. Rossbach[6]

Sweden is today exposed to information operations that can affect freedom of expression and opinion. In the event of a so-called grey zone conflict (a conflict short of war), the amount of disinformation that is directed at the public and decision-makers will only increase. To defend itself, Sweden will need to organize its countermeasures more clearly and coherently, and increase its will to resist. Effective resistance nevertheless assumes the existence of a, currently non-existent, designated central authority able to undertake a modern strategic psychological defence, including to survey the entire array of threats as well as the roles and capabilities of the affected agencies. Without a cohesive psychological defence, government agencies risk passing the buck among themselves; and it will be very difficult to both resist attempts to spread disinformation and strengthen the will to defend. In the absence of such countermeasures, no other part of defence will be able to function.

Psychological defence is vital to Sweden's total defence effort

"I can fly. I am not afraid", says Stig-Helmer in the classic Swedish film, *Sällskapsresan* (The Charter Trip). Just as Stig-Helmer needs to reassure himself that it is safe to fly, the Swedish public needs to be reassured that it is meaningful to defend the country in the event of a conflict. This applies even in the so-called grey zone between peace and war, when an enemy is trying to influence events short of direct acts of war. A coherent effort will be needed to maintain this conviction, and this is something to which strategic psychological defence can contribute.[7]

[6] The article is based on research carried out at the University of Oxford, supported by the Axel and Margaret Ax:son Johnson Foundation.

[7] The concept of 'psychological defence' was established in Sweden as a practical response to preparations for psychological warfare being undertaken in the rest of the world, with the publication of the official government report, SOU 1953:27 *Psykologiskt försvar* [Psychological defence]. Today, the term is often used to cover many overlapping concepts, such as responses to disinformation operations, morale-boosting and resilience-enhancing operations, and information warfare or PSYOPS.

Without a robust psychological defence, Swedish values stand unprotected against hostile actions that seek to influence Sweden's decisions and actions. This in turn risks undermining both civil and military efforts to defend Sweden. Psychological defence is thus a fundamental strategic concern that involves the entire total defence effort.

Psychological defence is just as central for the new total defence as it was during the Cold War. For most of the past few decades, however, work on psychological defence has been significantly reduced. Increased security tensions in Sweden's near abroad, however, have made it necessary to pay attention to the important role of psychological defence in the defence of Sweden.

Psychological defence: a durable concept

Sweden's psychological defence was originally a response to the psychological warfare the enemy was expected to carry out in the event of war. The term 'psychological defence', primarily used in Sweden, was established in an attempt to move away the older and more specific term – propaganda – which is primarily associated with Nazi Germany and the Second World War. The Swedish term has shown itself to be sustainable and adaptable, but its meaning has become blurred, especially since its applications concern several government agencies. Nevertheless, psychological defence has outlived all conceivable competing concepts.

Psychological defence has three essential components. However, the prominence of each of these has varied over the years. The three parts are:

- to counteract deception and disinformation, including rumour-mongering and propaganda or, in other words, everything that hostile psychological warfare engages in;
- to ensure that the government authorities can get their message out in a crisis, including war;
- to contribute to strengthening the population's will to defend Sweden.

Novel technology has always been employed in the service of psychological warfare. Hardly ten years after Nazi Germany's propaganda minister, Joseph Goebbels, made his last radio broadcast, Swedish psychological defence was experimenting with live television press conferences about its exercises, with the aim of protecting democracy.

Psychological warfare can occur through various means. In addition to disinformation, it can also make use of diplomatic and economic means. Modern information and communications technology in the cyber arena provide new opportunities for psychological warfare. False news can be disseminated through social media and cyberattacks on Swedish infrastructure could, together with the use of rumours, undermine the public's confidence in the authorities. Sweden needs a coherent overview of all the potential ways in which an enemy might launch propaganda and information operations. It is also important to understand how the threat has changed since the Cold War.

New and old threats

The prerequisites of psychological warfare were completely different during the Cold War. Then the threat was more straightforward, with one enemy and one type of conflict, whereas today there are many kinds of threats. Psychological defence activities must now deal with both state and non-state actors and, while counteracting operations that occur in peacetime, must be prepared for wartime conditions. The similarity between the past and the present lies in the fact that it is the same vital values that are at stake, such as free elections. Previously, democracies risked becoming victims of an occupying power. Today, a foreign power may instead attempt to manipulate Swedish political elections through various kinds of information operations.

Then as now, the will to defend was central to a functioning defence. A defence requires both the will to act and the capability to do so. Taken to its extreme, without the will to defend Sweden all the equipment and all the armed forces will be of little value. Ensuring sufficient motivation, however, cannot only be the responsibility of a strategic psychological defence.

Achieving and maintaining the will to defend requires action from several distinct parts of society, not least the various government agencies. In their efforts to strengthen the will to defend, however, there is a risk that a government agency, unintentionally or otherwise, might lapse into some form of domestic propaganda, which could do much more harm than good. Strengthening the will to defend is an issue that requires careful consideration of the roles and responsibilities of government and those of other parts of society.

In the 1950s, the National Preparedness Commission for Psychological Defence (the predecessor of the National Board of Psychological Defence, SPF) wished to avoid being accused of any form of manipulation of the public. During the Second World War, Sweden used its fair share of clumsy and politically doubtful measures for managing public opinion, and the new organisation for psychological defence wanted to avoid being associated with them. Nonetheless, a psychological defence exercise held in the 1970s, which drew much attention and some saw as an exercise in domestic propaganda, reminded decision-makers of the risks. Even in the 1980s, when peacetime tasks such as providing information on total defence became part of psychological defence, decision-makers feared that this might become problematic.

Today, total defence may need a new narrative about what constitutes a credible defence. Such an account would certainly need to be formulated, or at least affirmed, politically, not least in order to show how government agencies are working together in a meaningful way. A strategic psychological defence would be able to coordinate a narrative about the values that Sweden wishes to uphold, especially regarding security-related matters.

Without a coordinated psychological defence, it is likely to be more difficult to ensure a will to defend. The will to defend must be reinforced before a crisis breaks out, and is required to help explain the need to build and participate in a total defence. The will to defend is also important in order to advance the recruitment of civil defence and armed forces personnel, and especially to justify conscription. The will to defend has traditionally been defined by Cold War conditions, and the assumption that the threat is an armed attack by a foreign power. For information operations in peacetime, it might also be necessary to ensure the will to defend, or to establish a new type of will to defend, against low-intensity threats.

Psychological defence in the future

The psychological defence activities of the Swedish Civil Contingencies Agency (MSB) can be viewed as peacetime "here and now" tasks, which psychological defence during the Cold War only engaged in to a limited extent. Psychological defence during the Cold War was certainly strategic, but its role in preparing the population during peacetime for how it should act in the event of war was limited.

Some parts of the MSB's tasks stem from the old psychological defence. The MSB studies not only developments in the public's will to defend the country, but also public opinion on propaganda and grey zone conflicts. The agency has increased its knowledge about information operations and how Sweden might defend itself. This type of activity is likely to become ever more important due to so-called hybrid warfare. If propaganda and information operations are sufficient to allow the enemy to achieve its objectives, allowing a conflict to escalate to a war would serve little purpose. But also even an enemy that is preparing for war would want to undermine Sweden's will to defend itself before an open conflict broke out. Research and knowledge about an adversary's methods is not enough to strengthen the will to defend. A clear division of responsibility among all the government agencies is also required.

If the tasks of psychological defence become the responsibility of many different government agencies, there is a risk that psychological defence will devolve into disparate efforts and become nobody's responsibility. Some authorities might treat it as a technical task connected to cyber and IT issues, while others might not make it a priority. As long as the threats are low-intensity, they can perhaps be dealt with separately without a single coordinating authority. In a crisis, however, it will become apparent that more is required than just a network of agencies dealing with psychological defence based on their own separate needs.

The number and types of threats have changed since the Cold War. This increases the need for a coherent view and is one reason why a central authority is needed – a strategic psychological defence body preferably in the form of a separate agency. Psychological warfare can be conducted in several ways, but to counteract them successfully it is important to be able to understand an opponent's information operation within a larger strategic context.

The armed forces have a vital role in psychological defence, and have capabilities for engaging in psychological operations (PSYOPS), for example during overseas military operations. This is nonetheless very different from the strategic psychological defence that Sweden had in earlier times. Such a defence should not be coordinated by the armed forces, just as was it not during the Cold War. First, because it would be problematic if questions that concern the heart of Sweden's democracy, such as the freedoms of expression and opinion, were subjugated to military considerations. In addition, such threats already exist in peacetime; and in the event of war the armed forces must focus on tactical psychological warfare at the frontline, and hence cannot take responsibility for the whole of society.

In sum modern, a well-functioning total defence would probably be best served by a centrally organised psychological defence that is clear and cohesive; that is, a strategic psychological defence. This would mean a combination of the status that psychological defence had during the Cold War and the tasks that today fall within the framework of psychological defence at the MSB.

A strategic psychological defence is necessary

To understand the need for a modern psychological defence, it is not necessary to scrutinize military scenarios. It is merely necessary to highlight the risk that information operations could undermine the country's democracy and capacity for decision-making in the event of a crisis. Today, psychological defence is needed to fight the effects of information operations in peacetime, not just in war. Psychological defence could even be a decisive instrument that averts the threat from an enemy that is unwilling to escalate a conflict to a war.

For psychological defence to be effective it must be strategic. This is true for three reasons:

First, a concise, comprehensive knowledge of an enemy's methods of psychological warfare is required. A reasonably skilful handling of information operations in key parts of society, such as the media and intelligence agencies, is insufficient. In the event of a sudden crisis or a serious conflict, a concise, comprehensive grasp of the aims of information operations and how countermeasures can be swiftly organised could prove crucial.

Second, it is necessary to consider giving special status to psychological defence within the framework of the new total defence effort, not least to show where psychological defence matters are being coordinated. Officials in Sweden, as much as the public, need to know where to go for help in identifying psychological warfare and where they will receive support in countering it, whether the influence is directed at a municipality, an individual or the entire country. Without a strategic and central status for psychological defence, its objectives risk being lost among several different government agencies. Strategic psychological defence should, as before, have a clearly civil status in order to guarantee it autonomous role within the framework of total defence. This would also facilitate collaboration on an equal footing with the intelligence, defence and other government agencies.

Finally, strategic psychological defence would make it easier to collaborate and demonstrate solidarity with other similarly inclined countries. These countries would know which Swedish authority they would be collaborating with on joint measures to defend against psychological warfare. A strategic psychological defence would also make it easier for Sweden to suggest which values should be given priority internationally.

Further Reading

Niklas H. Rossback, (preliminary title) *Fighting propaganda: The Swedish Experience of Psychological Warfare and Sweden's Psychological Defence, 1940–1960*, forthcoming, Axel and Margaret Ax:son Johnson Foundation.

7. The Internet as a Military Arena: a Challenge for the New Total Defence

Mikael Wedlin and Erik Westring

There is a fast growing dependence on the Internet for critical societal functions. New services are constantly being developed to replace existing ways of communicating. This has increased the significance of the Internet from a defence-related perspective. Intelligence gathering and influence operations, as well as covert military operations, are areas in which even in peacetime, the Internet has been used as new military tool. The digital battlefield will therefore be of major importance in the development of modern total defence. It is vital that Sweden stays abreast of the latest technical, organisational and legal advances.

That the Internet can also function as an arena for military activity is not a new idea. When FOI began to study IT warfare in the second half of the 1990s, research proceeded on the assumption that this would be the future of warfare, and that mines and missiles were history. Especially worrying was the expectation that our critical infrastructure could be digitally influenced or seriously disrupted. Now that Internet operations have become a reality in ongoing conflicts, it is possible to determine what a realistic future might look like. We were correct in guessing that the Internet would become a major part of daily life; no part of life today is untouched by Internet-connected systems. The influence of the Internet arena on current conflicts, however, has not created digital attacks that knock out entire societies, as was feared. Instead, it is in the phase immediately prior to an armed conflict that the Internet has been used most.

Even if we are now beginning to understand the mechanisms of warfare on the Internet, it is still extremely difficult to predict the future of the Internet as a whole with any precision. The first Swedish Internet bank began in 1996, but it is only in the past five to ten years that the Internet has become the *de facto* foremost communications channel for banking transactions. Almost all the services that we take for granted today, such as Google, Facebook and YouTube, were created in the past 20 years. It is possible to predict with a reasonable degree of certainty, however, that the Internet will continue to be significant for all sectors of society, and that its significance will probably increase. One could even go so far as to claim that the Internet will eventually lead to greater changes in lifestyles than those brought about by the Industrial Revolution in the nineteenth century.

The military challenges

Four of the Internet's characteristics create major defence and security policy challenges and specific military problems:

Anonymity on the Internet makes it relatively simple to conduct easily deniable operations. On the Internet, it is difficult to be certain that someone is really the person they claim to be. The legal legitimacy of a military intervention applies only if one can associate a military state actor with an activity, something that can be fundamentally difficult on the Internet. From a military perspective, this is an advantage if the aim is to act covertly and a disadvantage if seeking to defend oneself.

Thanks to the Internet, military operations can be conducted from a great distance. The Internet is a domain completely without national borders and "movement" can in principle be immediate and without distance. This means that operations on the Internet can be carried out from anywhere and, in principle, without any risk to military personnel. The absence of borders also gives rise to judicial ambiguity with regard to international law. Is placing malicious code on a mail server in a third country using someone else's territory?

The civil and military digital arenas share the same infrastructure. Military and civil threats have previously been separate. Sweden, in particular, has traditionally taken great pains to create a clear separation. On the Internet, however, military and civil threats flow into each other. This is particularly the case since it can be difficult to determine the origin, purpose and goal of an attack. If all the country's banks are suddenly taken down simultaneously, the antagonist may be another state conducting an act of war or a group of bored or politically motivated teenagers. Such events are generally difficult to evaluate or analyse quickly. It is also difficult to determine which laws, if any, apply to IT attacks. Most of the conflicts in the Middle East have been accompanied by intrusions into web servers. Is this part of a military operation? Who is accountable? Does it make any difference if the sender is military? Sweden's greatest challenge is to achieve a division of labour between the armed forces and civil defence.

The Internet opens up cost-effective opportunities for asymmetric warfare. Attacks on the Internet are often of an asymmetric nature. Even small, financially strapped organisations or individuals can carry out acts on the web. The ability to conduct Internet attacks is entirely knowledge-based and a single individual with the right competences can disrupt even relatively large systems. Nonetheless, even on the Internet, generating large-scale disruption or long-term damage requires more substantial resources in the form of both intelligence capacity and time.

A clear example of this is *Stuxnet,* the attack on Iran's nuclear programme which was carried out by a computer virus targeted at the uranium enrichment facility in Natanz. A virus planted in the control systems destroyed a number of centrifuges and left the facility unable to enrich uranium. At the time of its discovery, this malicious code was among the most advanced ever seen. It was assembled from various different types of code written by several different programmers. With enough knowledge and time, however, it could have been written by a single person. To create successful code of this targeted type requires intimate knowledge of Iran's nuclear programme, detailed blueprints and access to both the hardware and the software one wants to attack – in this case, centrifuges – as well as the frequency converters that control them. The latter is essential to be able to develop malicious code that will destroy the centrifuges without triggering their in-built defences. Access to resources such as these is today only available to states.

Even if the Internet makes asymmetrical warfare possible, it is unlikely that someone with limited resources could achieve more than minor disruption. A strike against an entire sector of society would require a highly qualified adversary.

Fields of application of the Internet as military means

Traditional military means will still usually generate greater and more predictable effects than a cyberattack. For instance, the cyberattack on Ukraine's electricity supply during Christmas of 2015 was planned at least six months in advance and created a brief disruption, but the first subscribers had their electricity supply restored after a three-hour interruption. Traditional aggression against Ukraine's electricity supply would probably have caused more permanent, as well as more predictable, damage. The use of cyberattacks to cripple infrastructure is therefore likely be a complement to traditional capabilities. There are three areas in particular where the Internet is a particularly relevant arena for military operations:

For intelligence gathering. The Internet must be every intelligence organisation's dream. Information is located in a single location that is relatively accessible, and available in a format that can be gathered and processed automatically. It is evident that this is already happening on a massive scale, and that substantial resources are being allocated to information collection. An obvious example of this is the Snowden case, and the disclosures that resulted. There are also numerous published examples of illegal monitoring of organisations and individuals by the Chinese state.

As a platform and means for Influence Operations. The Internet has changed media habits and news-gathering methods in a fundamental way. Today, anybody can be a producer of information. Even in the well-organised information environment of the recent past, with only a limited number of information providers, it was difficult to identify a source. In today's media environment it is nearly impossible. False information that seeks to influence opinion can be spread with the efficiency of an epidemic. The flow of information is becoming an avalanche and actors in our neighbourhood are rearming in a goal-driven way on the Internet to use new digital media for their own geopolitical purposes. The 2016 presidential election in the USA is a worrying example. It is highly probable that future European elections will be exposed to the same kind of influence. The disruption of Ukraine's electricity supply in 2015 can also be considered an influence operation, which was probably done to instil feelings of insecurity in the population rather than further any traditional military goal. The Internet has therefore ushered in new, more effective methods and tools for influence operations, and there is every reason to assume that their scale will continue to grow.

Covert operations in the grey and twilight zones. Deniability in Internet operations can be used in situations where a military operation is required but it is important that it is not understood as an act of war. The above-mentioned example of *Stuxnet* is typical of this category. It was an extremely advanced operation, but it is safe to assume that the sender did not want the hostilities to escalate into open conflict. Actions on the Internet also have a special significance in preparations for war and so-called pre-combat. In conclusion, it seems likely that the military uses of the Internet will affect populations most in peacetime.

International outlook

Several states have recently openly declared that they are in possession of a military Internet capability. This strengthens the assumption that the Internet will become a natural part of future military conflicts. Several times in recent years, for example, Russia has been accused of using data intrusion as a method of conflict. The *Stuxnet* operation was probably conducted by the USA and Israel, although neither has admitted this. China and Iran, among others, have also appeared in intrusion reports where it is reasonable to assume that a state actor lies behind the intrusion.

States have recently been shown to be very interested in information about other countries' infrastructure. Reports by US governmental organisations cite evidence that the USA's infrastructure has been mapped by foreign states. Sweden's National Defence Radio Establishment (FRA) reports that more than 10,000 "cyberactivities" are being directed against the country every month. According to the FRA, although the overwhelming majority of these are purely spying or other efforts to access information, at least one attempt to map Sweden's infrastructure has been identified.

After Estonia was heavily exposed to IT attacks in the spring of 2007, it established the Estonian Cyber Defence League, something resembling a "digital home guard". The aim is to strengthen society's capacity to deal with cyberattacks and to set up public-private sector partnerships.

Where does Sweden stand today?

Sweden has a relatively high degree of computer literacy and has worked actively to strengthen the general level of IT security over the past ten years. Thus, in international comparisons of risks linked to IT threats, Sweden does relatively well. Our critical infrastructure, on the other hand, is not constructed to resist attacks, in either cyberspace or the real world, from an entity with the resources of a state. There is still much to do.

The primary objective of FOI's work on IT security has been to raise awareness and introduce protections against the simplest types of attack. IT security has been a small area of research relative to the speed of developments in the IT field more generally. Maintaining attention on security aspects can be a challenge in a period of such rapid development. There is a major need for more advanced research.

Changes in the global situation in recent years have led Sweden to begin to reconstruct its civil defence, and the concept of total defence has gained new relevance. The societal change associated with the Internet has occurred since Sweden last implemented total defence and the new total defence set-up will have to include defences against digital threats.

The roles for managing digital threats need to be clarified. Whose job is it to put out fires on the Internet? If foreign military flights violate Sweden's borders, the Swedish Armed Forces scramble their own aircraft to intercept them. If a German freight train loaded with chemicals derails outside Stenungsund, it is the police and the fire department that deal with it. In the Internet world it is different, not least because civil and military threats blur into each other.

Sweden's resilience against digital threats will depend on how everyone in society collaborates. Collaboration already exists between the defence authorities and the crisis management system but must be developed further. In example, more explicit collaboration between the police and the military authorities must be forthcoming, and the opportunities for the armed forces to support the police must be expanded. In addition, civil suppliers of critical societal functions, such as mobile phone operators and banks, must be involved in planning for and managing threats. This is a major challenge for total defence.

Influence operations on the Internet constitute a clear threat to democracy and our political processes. It is obvious that during the construction of total defence we must also build competences and develop technologies to help understand and detect these attacks, to enable us to effectively oppose this type of subtle warfare. This type of external influence is already happening.

National and international regulation will be required to deal with digital threats. It will remain a challenge, however, to regulate such a rapidly changing area. At the same time, it will also be important to protect openness on the Internet. Sweden has a role to play in standing up for a type of openness that facilitates accountability. In the same way as there is a fire department to respond to fires that an individual cannot handle alone, maybe we need a force of volunteer IT technicians that has undergone training and is prepared to act in a crisis in a way that an individual system owner cannot when facing a major disturbance that it cannot handle alone. Does Sweden, like Estonia, need a digital home guard?

8. Internet of Things: an IT Security Nightmare

Daniel Eidenskog and Farzad Kamrani

Internet of Things (IoT) is the collective name given to products that contain electronics that have some form of connection to other systems, usually via the Internet. The number of cyberattacks involving IoT devices has increased in recent years. This, combined with a deteriorating security situation, presents a looming risk of major and wider cyberattacks in which IoT devices will be central. Sweden's national security and system of total defence are built to a great extent on the resilience of critical societal functions. Many of these have Internet-connected systems that are partially based on IoT products, making them vulnerable to cyberattacks. These systems are clear targets for antagonists. To reduce the risk of serious cyberattacks capable of disrupting critical societal functions, Sweden should have a clear strategy on cybersecurity. Sweden should also take an active role in efforts to increase cybersecurity in commercial IoT products.

A growth market with little security focus

Internet of Things (IoT) is a huge market that comprises products from a range of different sectors, such as household appliances, vehicles, building systems and industrial machines. The rate of growth of the IoT market has been high and market analysts are predicting a global increase from approximately five billion devices in 2015 to at least 75 billion by 2025. Market analysts also predict that individual consumers will own the majority of these devices. Cybersecurity is not an important criterion for this customer base, neither at purchase nor during use. New features and low prices are more often the deciding factors. In addition, there is no formal regulation of the cybersecurity aspects of IoT products and it is difficult to make the manufacturers accountable for vulnerabilities in their merchandise. In general, manufacturers have few incentives to improve cybersecurity. In many cases, this leads to products with a level of security that is far below that in many other information technology related areas.

Security is often inadequate even in IoT devices targeted at professional users. Extensive vulnerabilities have been demonstrated for example in professional-grade surveillance cameras. In several cases, these flaws have indicated a total absence of even a basic understanding of cybersecurity when developing the software for the devices.

The substantial number of IoT devices and the lack of security indicate a risk that any cyberattack that targets or seeks to take advantage of IoT products would have the potential to become a large-scale attack. Such extensive attacks would be likely to affect the infrastructure of the Internet, potentially critical societal systems and individuals.

National security is dependent on the Internet

Sweden's system of total defence relies on the assumption that normal societal services will be capable of maintaining a functioning society even in the event of a crisis or war. This applies to both military and civilian functions where disruptions and disturbances would have far-reaching operational consequences, which by extension could affect the whole of society. Fundamental societally critical sectors such as the drinking water supply, the energy supply, food distribution and communications all rely on IT systems as well as industrial control systems.

Many systems in critical sectors have connections to the Internet and build at least partially on IoT products. This puts these systems at risk of cyberattack. In the current global security climate, there is a risk that ever greater and wider attacks will be carried out against critical societal functions, where the attacks target IoT products or where IoT products are used as a springboard to amplify the attacks.

Sweden's high dependence on IT means that society is exposed to cyber-risks that would have been unimaginable only two decades ago. This dependence on the Internet as infrastructure, along with vital societal functions at risk of cyberattack, make the potential consequences of a widespread cyberattack huge.

To reduce the risk of serious cyber incidents and their subsequent disturbance of critical functions, Sweden must actively work to improve cybersecurity in the IoT:

Sweden should have a clear cyber strategy that aims to increase awareness and readiness. An important part of such a strategy should be to clarify the importance of the systems and components that the state does not control. The so-called proximity principle in the Swedish crisis management system puts local authorities in charge of managing a crisis. The fact that it is relatively simple to conduct a cyberattack from a distant location makes this principle ill-suited to handling a crisis resulting from a cyberattack.

Sweden should take an active role in efforts to increase cybersecurity in commercial products, for example as part of EU cooperation. Cyber security issues are basically global for all systems connected to the Internet, which means that improving cybersecurity must be pursued at both the national and the international levels. The cybersecurity situation in the private sector affects society and must therefore be part of the state's efforts in the cybersecurity arena.

Privacy is greater than the person

Another aspect of the widespread presence of IoT devices involves privacy, which by extension can also affect national security. The purpose of many IoT devices is to collect information about the user, for example in the form of places visited, health status, training habits or other activities. Devices usually send information to the manufacturer's cloud services to enable the user to easily access and use the functions provided by the services. However, these functions also give the manufacturer access to the information.

A fundamental problem is that IoT products introduce many new risks to privacy, often at a faster rate than legal mechanisms and social norms can adapt. In a world where more and more things are connected to the Internet, the cost of collecting, storing, processing and sharing data is shrinking dramatically. These privacy risks extend from simple, everyday problems, such as overprotective parents monitoring their children or intrusive marketing, to more serious cases, where governments and state actors limit the freedom of their citizens or carry out attacks against other countries.

The richness of the information that is accessible through IoT devices, combined with increased computational capacity and more effective algorithms, have created enormous opportunities for identifying, surveying, eavesdropping on and tracking individuals, as well as mapping their behaviour patterns. IoT devices often use passive methods of data collection, which means that users are usually not aware that they are being watched.

People in key positions in society risk being subjected to targeted attacks using, among other things, IoT devices. Targeted attacks against individuals are usually carried out with the assistance of well-informed and sophisticated social engineering combined with technical means. The British journalist and human rights activist, Rori Donaghy, was subjected to such a targeted attack, through a combination of social engineering and malicious code. Successful social engineering requires the attacker to have thorough knowledge of the victim, which the attacker can obtain by gathering information from diverse sources. By attacking IoT devices and potentially gaining access to large amounts of data, an attacker increases its chances of success against specific key persons.

Surveillance through bugging or tapping has long been a method for gathering just the type of information described above. One major obstacle has always been the difficulty of placing suitable listening devices close enough to the target. The dramatic increase in the number of IoT devices increases the quantity of devices that could be used for listening. In addition, the IoT devices are voluntarily put in place by the very people who are being monitored. Examples of devices that can be used for this type of surveillance are IP cameras, computers, smartphones, smart watches, wireless headsets and voice-controlled devices in homes.

Large numbers of vulnerabilities and attacks

Cyberattacks can be used to target information systems, computer networks and personal computers. The IoT – in the form of sensors, actuators, control systems and everyday objects – is increasingly interweaving the physical world with the Internet, thereby enabling new types of attack. IoT devices allow an adversary to take control of physical objects and cause physical destruction or even loss of life. The *Stuxnet* worm, which was aimed at nuclear enrichment plants in Iran, the 2015 attack against Ukraine's electricity grid and examples of researchers taking total control of a car through its Internet connection show that attacks against IoT devices encompass completely new dimensions.

The vulnerabilities in installed products are seldom addressed, since in many cases installing updates is a complex procedure that must be performed manually by the consumer. In addition, it is common for products to still be in use several years after the manufacturer has stopped releasing security updates, which makes it impossible for the consumer to avoid security defects.

Denial-of-service attacks that use IoT devices have increased in number in recent years and produced some of the most powerful disruptions of the Internet to date. In October 2016 a denial-of-service attack was directed at a core function of the Internet: a provider of the Domain Name System. It left a number of websites inaccessible to most users for several hours. Among the affected websites were Swedish government sites – krisinformation.se and regeringen.se – as well as several commercial and news services, such as Netflix, Spotify, Twitter, the BBC, CNN and Fox News. This denial-of-service attack, like several other extensive overload attacks, was based on malicious code infecting large numbers of IoT devices.

Many attacks lead to the attacker gaining complete control over an entity and its information. When the goal of the attack is the person or organisation using the IoT device, the attack can be much more subtle than an overload attack. It has, for example, been shown to be simple to hide an event by manipulating the video stream delivered by a network-connected surveillance camera.

When parts of Ukraine's electricity grid were shut down by an extensive and advanced cyberattack in December 2015, although it relied almost entirely on vulnerabilities in traditional IT systems, it also included attacks against IoT-like devices. During the attack, the attackers replaced software in certain components, causing communications with facilities to cease to function. This meant that restoring electricity distribution required manual actions to be carried out on site, and that parts of the grid could not be remotely controlled until the affected equipment had been replaced.

Destructive attacks have also occurred on the Internet using malicious code that targets certain IoT devices, leaving them unusable. There has been speculation about the actual target of these attacks. One theory is that the attackers are targeting manufacturers in the hope that they will be negatively affected by warranty claims and bad publicity. The purpose of these attacks thus being to increase the incentives of manufacturers to develop more secure products from fear of losing customers.

Attacks where the objective is to access the information in the IoT devices are often directed against individuals or organisations – opportunistically or randomly selected – from where information can be gathered or whose systems can be taken over for purposes of extortion, mapping or surveillance. Products that are increasingly present in private homes, such as network-connected surveillance cameras and baby monitors, have been highlighted in the media. Security defects have also been observed in a broad spectrum of products, such as smart televisions, insulin pumps, toys, home appliances, industrial dishwashers, thermostats, cars and sex toys.

It is extremely important that IoT manufacturers gain knowledge of the vulnerabilities of their products and rectify them. Some state actors collect information about vulnerabilities for their own intelligence activities rather than reporting them to the manufacturers or making them more generally known. This tendency is highly worrying, since there are no guarantees that such knowledge will not leak and damage the public interest, as occurred when a leaked vulnerability was used in a widely distributed blackmail virus.

Cybersecurity lacks instruments of control

There are currently no instruments for improving cybersecurity in commercial products. Customer demand in the cybersecurity area remains low, especially in consumer products as many types of attacks, such as denial-of-service attacks, do not affect the people who own the equipment. That said, the increased media focus on cyberattacks and vulnerabilities might raise consumer awareness of the impacts of inadequate cybersecurity, and with it the demands they make of manufacturers.

There are discussions at the EU level about introducing a "trusted IoT label" for IoT products that meet certain security requirements. This is meant to build on the same principle as the energy labelling of domestic appliances, where the specifications are clearly presented for the consumer to direct them towards safer or more energy-efficient products.

An alternative route would involve legislation and regulation. One possibility would be to design regulations similar to the system of mandatory CE-labelling of products sold within the EU. CE-labelling places greater responsibility on the manufacturers and importers of products, this has generally worked well, although some fraudulence still occurs when products are CE-labelled even though they have failed to meet the regulatory requirements.

As long as the current lack of incentives for producers persists, however, there is every indication that the problems caused by inadequate cybersecurity in the IoT arena will continue for the foreseeable future. As the number of installed IoT devices increases, the consequences of insecure IoT will continue to increase.

Further Reading

Farzad Kamrani, Mikael Wedlin and Ioana Rodhe, *Internet of Things: Security and Privacy Issues*, 2016. FOI-R--4362--SE.

9. The Swedish Electricity Supply System: How to Deal with Increasing Vulnerability

Maria Andersson and Lars Westerdahl

Society has become totally dependent on electricity. Without it, many daily activities could no longer be performed. The electricity supply system is vulnerable, however, and the ongoing transition to smart grids will make it even more so. Cyberattacks can be carried out even on the existing power grid. These attacks cause major disturbances to society, as was demonstrated by the recent cyberattack on Ukraine's power grid. These increased risks must be taken into account in the ongoing transformation of the Swedish electricity supply system.

The electricity supply system as a target for cyberattacks

Suspected preparations for cyberattacks on the Swedish power grid have recently been reported. Sweden's National Defence Radio Establishment (FRA) announced in January 2017 that it had detected suspicious activities and preparations. The 2015 cyberattack on the Ukrainian power grid began with emails being sent to several electricity distributors. The emails contained attachments with malicious code that made it possible for the attackers to pass through firewalls and into the control system. Hundreds of thousands of electricity customers lost power while the power grid had to be manually restarted, which took several hours.

The evolving power supply system

The Swedish power grid is evolving into a so-called smart grid. Smart grids are characterised by increased use of modern communications technology. Data is collected from more actors, which creates opportunities for detailed analyses of different states in the power supply system. These analyses can serve as a basis for more cost-effective pricing, improved demand forecasting and higher demand flexibility. Smart grids provide good opportunities to improve energy efficiency and reduce costs in the power supply system. However, the transition to smart grids also increases vulnerability to cyberattacks.

Traditional power grids distribute electricity in one direction and production is adapted to a standardised customer demand.

From a historical perspective, electricity production has mainly taken place in large-scale power generation plants, such as hydroelectric or nuclear power stations. Smart grids can be seen as an upgrade on the traditional grid, where new technologies are installed to improve control and monitoring in all areas of the power supply system – the production, transmission and distribution systems – as well as with the customer. To make full use of the benefits of the new technology, several actors need to be able to communicate and interact. The new technology makes it possible to better balance electricity supply and demand. Smart grids can react better to demand flexibility and the variable electricity production of renewable energy sources such as solar and wind power in local energy systems. Another driving force behind the transition to smart grids is climate policy. Climate targets in the European Union and Sweden require reductions in greenhouse gas emissions. Key elements of achieving climate goals are an increase in the use of renewable energy sources and improved energy efficiency, both of which will benefit from the move to smart grids. In summary, the large-scale introduction of variable electricity production, energy efficiency measures and demand flexibility will create demand for improved monitoring, control and measurement in the grid – the technologies that characterise smart grids.

Increased vulnerability

The grid control system has traditionally been more or less isolated from the outside world. Developments in IT, however, as well as cheaper IT components mean that traditional electrical components and vendor-specific solutions are being replaced in control systems with hardware and software components as well as communication protocols that were initially developed for ordinary office systems. This has resulted in control systems and office systems being able to communicate with each other. For the electricity providers, this has meant a potential increase in the availability of up-to-date information on what or how much is produced. This information can be used, for example, to charge the customer more accurately.

This interconnection of systems has not only created an increased need for communications. Interconnected systems also increase the exposure of production, transmission and distribution systems to an environment that they were not designed to handle. Increased internal communication will increase the complexity of the power supply system. At the same time, however, increased exposure to the Internet will leave systems open to hostile intentions. An antagonist, that is, a conscious attacker who wants to steal information, prevent access to systems or exploit such systems for their own interests, is something that did not previously need to be considered to any great extent.

Correctly implemented security functions are difficult to get past. This means that attackers rely instead on *phishing* and *spear phishing*, which aim to trick a person sitting at a computer in the target organization into opening a prepared attachment or clicking a link to a prepared web page. If the person opens the attachment or clicks the link, the attacker has passed the firewall and entered the network. Based on such a foothold, an attacker can move on to the main goal.

The need for structured security work

The risk of vulnerabilities increases in complex systems with multiple actors. In such an environment, structured security work between actors is required to achieve adequate protection for the entire power grid. Each actor needs to work systematically on security issues for their own system throughout the lifecycle of the system. Security is not a product that is installed once, but rather the result of continuing work.

The aim of security work is that a system should be able to contribute to the operation even if antagonists try to attack it. This is achieved by a combination of training for staff, administrative measures and technical solutions. Continuous security work is particularly important for control systems, given that they usually have a long service life, sometimes of up to 20 years, and high availability requirements. This is in comparison with office-based IT systems, which are usually replaced every three to five years.

A system is designed to handle known vulnerabilities. As the system is maintained and adjusted, new vulnerabilities may arise, for example through increased exposure. A system that is not maintained from a security perspective will deteriorate over time.

Security analysis

Infrastructure systems such as power supply systems are rarely developed by a single system owner. Several actors interact within the power supply system, and the system consists of several subsystems with interdependencies. Changes in these subsystems do not occur at the same time, which means that new and old subsystems will need to exchange information. The subsystems may also have dependencies between them.

Building IT systems in an environment where there are multiple systems with different owners places great demands on the interfaces between the systems for enabling communication. Each actor must ensure the functioning of its subsystem and identify the risks to which the subsystem is exposed. It is therefore important that subsystem owners share a common view of the threat situation in which their systems will operate. When a new system is to be introduced, security analysis is an important tool for identifying which security functions are needed and the procedures required to support them.

However, since the security of a system will deteriorate over time, security work does not end when the system is put into operation. IT systems contain weaknesses that are detected as the system is used and corrected by *patching*. If patching is not performed, the system will contain known weaknesses.

A managed system will constantly change. This means that continuous security analyses need to be conducted. The functionality assigned to a system after it has been put into operation needs to be examined as carefully as new functionality is examined during system development.

To prevent cyberattacks

The foundations of and prerequisites for the security of a system are installed during system development and reinforced through maintenance work. However, active security work is also required during the system's operation, including preemptive and follow-up activities over time. Increased security is achieved through technical solutions, administrative procedures and supportive management.

Administrative procedures provide structure for security work. Structured security work, however, must focus not only on the functionality that the system will deliver, but also on the functionality of the system. This means that the system owner must know what has been installed in the system, and either support all of its functionality or remove any unnecessary functionality. Maintaining control of maintenance work, including of installed updates, is part of security work.

In collaborative systems, for example in power grids where there are several actors, it is even more important to actively monitor your own networks. The security functions provided during the development phase are designed to handle the threats that existed when the system was developed. New threats may have occurred to a system that has been in operation for a while.

Existing security solutions cannot always detect or handle these new threats. It is therefore important to pay attention, for example, to changes in patterns of communication in the network. Monitoring is required to detect illicit activities on the network, but staff members are also needed to follow up logs and alarms. Monitoring includes logging, intrusion-detection systems and anti-virus programs.

To handle cyberattacks

Whether the aim is information theft, prevention of access or to utilize system functionality for the attackers own purposes, once detected an attack needs to be addressed. How this should be done depends on the type of functionality that the system is delivering. For an information system that has no hard real-time requirements, the system can be shut down for a while in order to manage the intrusion. For a system that supports critical infrastructure such as power grids, however, this is not always possible. In such cases, the attack must be handled while the system continues to support the activities of the organization.

The key to handling an attack effectively is preparation. A crisis group established around a number of key individuals with good knowledge of the business and a large network of contacts will be an important resource in such a situation. The group must be prepared. It should have reviewed a number of possible scenarios and drawn up action plans, contact lists, and so on. Dealing with cyberattacks need not be the sole purpose of such a group. It could also act as a "general troubleshooter" within the organization.

Larger organizations could establish a Computer Emergency Response Team (CERT), a specific group highly skilled in handling IT problems. Its task would be to restore a system that had suffered an attack as quickly and efficiently as possible, while also ensuring that the same problem could not occur again. A CERT is expensive, which means that there tend to be industry cooperation or national functions established as external resources that can support smaller organizations by providing technical skills and knowledge of known threats.

Smart grids increase the exposure of control functionalities, which provides a larger attack surface. However, this attack surface does not necessarily lead to greater demands on other security functions in the system. On the other hand, there may be greater priority placed on the ability to detect intrusions and to handle incidents. An increasing number of actors in the power supply system also place a higher priority on the coordination of security issues.

The new power supply system requires both new and old security solutions

There are several strong drivers behind the transition to smart grids. These are likely to speed the transition. Both intensive and structured security work are essential during the transition phase, and this work should continue throughout the entire lifecycle of the power grid. Active security work, where people, administrative practices and technologies interact, is a necessity for long-life IT systems. This means that active safety work is important for as long as the system is in operation.

The attack on the Ukrainian power grid in 2015 is a good reminder of this need. Although electricity supply was lost for only a few hours, the attack was in preparation for several months. It is common for cyberattacks to go undiscovered for several months, sometimes years, depending on the attacker's goal. In Ukraine, the attack began with a targeted phishing attack to get a foothold in the networks. A long period of surveillance of the networks followed, to find a way from the initial entry computer to the actual target system. It is during this period when active security work, including monitoring, might have detected the attack.

Industry-based and national monitoring functions cannot be more effective than the tasks they are given. The Swedish power grid, like much other critical infrastructure, is made up of several actors. It is important that incidents are reported to an organization capable of maintaining an overview.

The events in Ukraine also taught another important lesson: manual recovery functions are still important. Technicians were forced to revert temporarily to manual functions in order to restore electricity distribution.

10. Geographic Information: a Vital and Rapidly Changing Asset

Ulf Söderman, Simon Ahlberg and Gustav Tolt

The ongoing digitalization of society means that anyone will soon be able to acquire detailed geographic data. This is a complicating factor in Swedish crisis- and defence-related planning that needs to be properly addressed and calls for new approaches. As the data available to the public increases, so does the importance of, for example, maintaining control of classified information. The antagonist's perspective should also be taken into account in technical development, in an attempt to prevent future unpleasant surprises and ill-informed decisions. Geographic information is a vital resource in transition. A new strategy and way to relate to it are therefore required.

A revolution in geographic information

Reliable geographic information is a prerequisite for efficient crisis management and vital to military activities. The information is used for planning, exercises and the execution of operations. Historically, geographic information concerning territory, such as topographic maps, has been a strategic and meticulously protected asset. Knowledge of local conditions, intended to offer advantages vis-à-vis potential opponents, has been used for defence planning and subject to restricted distribution.

A minor revolution in geographic information is currently in progress. With the digitalization of the society have come novel technical systems for data acquisition, as well as improved infrastructure for the storage, processing and distribution of data, and the presentation of results. There has been a sudden increase in the use and distribution of detailed geographic information, which countries are no longer in control of or have exclusive access to. The increased availability of individual data sets does not necessarily mean increased security risks, but a completely different situation could arise if several sources of information were brought together or interpreted using the right background knowledge.

Digital geographic information for everyone

Detailed geographic information is no longer reserved for certain groups and its distribution is not as meticulously controlled as it once was. In the ongoing digitalization of society, the trend is for increased use and distribution of detailed geographic information, and an increasing number of voices can be heard demanding free access, usage and distribution. One example is the entrepreneurship that promotes the exploitation of this type of data, the development of which has in most cases been publicly financed.

Behind the above trends are strong technical developments. Modern sensor equipment can collect substantial amounts of detailed data with ease. Digital cameras produce sharp images, radar sensors measure over large distances and see through clouds, while positioning systems make it easy to associate acquired data with geographic locations. Moreover, sensors are constantly getting cheaper and can now be found extensively in modern devices such as mobile phones, drones and vehicles. Several large commercial companies, as well as the more niche, high-tech firms in Sweden and abroad, are compiling huge amounts of publicly available geographic information. There are also initiatives in which users team up to gather and organize geographic data and make it available free of charge. One such example is OpenStreetMap, a crowd-sourced initiative that offers free map data to anyone.

IT infrastructure is also currently undergoing rapid development, such as new, powerful systems for handling vast amounts of data. Systems based on artificial intelligence learn to recognize objects and events, find patterns and instantly adapt information according to our wishes. Furthermore, novel presentation systems are being developed that allow quick and simple visualizations of results. A modern example of this is Virtual Reality (VR) glasses, which provide the user with a new way of viewing 3D representations of the environment.

Geographic information is beneficial for society

We can only speculate about what constant access to up-to-date national geographic data will mean in terms of new services in the future. Detailed data, such as new elevation data from the Swedish National Land Survey (*Lantmäteriet*), acquired through the processing of aerial imagery, could become a key component of new applications in numerous areas. These might be used for forestry planning, optimizing the placement of solar panels or analysing how various different environmental indicators change over time. They could also, of course, be used for defence-related purposes. Many new products and services will also benefit from the ever improving and increasingly detailed data, which can then be used to improve everyday life. Data could be used to navigate self-driving cars or to visualize construction projects using so-called augmented reality.

Technical developments provide many new opportunities for innovative applications, but they are dependent on the availability of data. Among developers and end-users, there is increased interest in so-called open data, or data that is free to use, reuse and distribute. There is also a strong drive to promote economic growth, both regionally and nationally, through innovation and entrepreneurship. This could have significant socio-economic benefits, in terms of new products and services as well as an increase in the efficiency of existing businesses.

The municipality of Helsingborg recently made a large part of its data available to the public. In addition to basic geographic data, this included information on security-, police- and fire service-related events, as well as maintenance issues and comments from local people. The data is accessible on the Internet and available to download. Several applications – or apps – have already emerged from this initiative. Helsingborg is not unique in this respect and many other municipalities are already working on similar projects.

Similar developments are also in progress at the national level. The Swedish National Land Survey has promoted the idea for several years, and today part of its data can be downloaded and used freely, including detailed road and terrain maps. Various other authorities have made parts of their data archives publicly available. The Swedish National Land Survey wants to take things further, but is currently hampered by a business model that requires a significant proportion of its budget to be covered by fees for using the information. The authority has presented cost-benefit analyses regarding open geographic data and made requests to the Ministry of Enterprise and Innovation, concerning changes to its business model. Large parts of the Land Survey's national geographic information may soon be available as a free and easily accessible resource.

Open data could become a security threat

What are the consequences from a defence and crisis management perspective of the increased availability of and demand for geographic information? What might happen if anyone can combine and analyse completely new combinations of data sets? Is it possible – or even desirable from a societal development point of view – to try to restrict the trend for geographic data to become increasingly accessible? These are difficult questions that should be addressed at the national level. By tradition, Sweden is a technologically advanced and innovation-friendly country. Technological advances are quickly adopted and neither legislation nor risk management tend to be able to keep up with the drive to exploit and capitalize on new technologies. This situation can lead to overreactions and demands for prohibitions or restrictions on the use of new technologies. In the case of the rapid development of unmanned aerial vehicles and the possibilities they offer, for instance, when the risks of such platforms became apparent, and the use of cameras was seen as in conflict with laws on personal privacy, a court ruling stopped companies using them in their businesses. By considering possible problems in the development phase, preventive measures can be taken that avoid the need for legislation or prohibition.

Free and easily access to geographic information does not just bring advantages. It will be just as easily available to antagonists or opponents, and it is not difficult to imagine scenarios where it would prove useful in the planning of hostile acts. Possible paths for invasion could be analysed, locations suitable for disembarkation or airdrops identified and target coordinates for precision-guided weapons determined with a high degree of accuracy. In a worst-case scenario, a person or a group with hostile intentions could perform all the necessary planning of an action without physically visiting the location in question, which would risk attracting attention that might reveal its plans. In the near future, attacks may also be conducted using autonomous vehicles, programmed to act completely or partially on their own. Their movements to their final destination could be controlled with precision using detailed geographic information.

These new circumstances raise the need to consider our stance with regard to the new playing field that is emerging from a defence and crisis management perspective. In a military scenario, an opponent could have access to the same detailed information that we do and the means to use it just as efficiently. We must analyse the risks this involves and how it affects defence and crisis planning. In this context, both the protection and the use of the information must be addressed.

Open and private data in the wrong hands

It is important to note that technical developments are continuing and the situation may become even more intractable. Where this concerns open geographic information, or other types of publicly available data and services, it is possible to know what a potential opponent might have access to. A new problem arises when new applications are developed in which various actors combine publicly existing information with their own data and intelligence gathering. Countries with substantial resources have always gathered their own data and intelligence. The difference today is that increasing numbers of commercial businesses are becoming involved. Access to and the use of data are increasingly beyond the control of governments. Thus, the need to control information that is worth protecting is likely to increase.

One concrete example is the rapid development of self-driving cars. A vital component in this development will be a highly detailed and up-to-date database of geographic information. Every vehicle will have multiple sensors on board that sense and analyse its immediate surroundings and combine the results with information in the database on the current traffic situation to ensure that the car arrives at its final destination as safely as possible. The sensor data collected is also used to update the database with the latest information from along the route. With contributions from hundreds of thousands of cars, the database will quickly become a dynamic, incredibly detailed, up-to-date 3D map of the road network infrastructure and its surroundings, while also providing information on the current traffic situation. All this information will probably also ensure a smoother flow of traffic. Traffic jams will automatically and quickly be detected and road users given help to plan their routes to minimize delays.

However, questions should also be asked such as how a criminal might be prevented from using the system to assist their system escape. If the police were to shut down public transport and block roads, this would immediately affect the traffic flow. A system programmed to maintain a smooth flow of traffic and help road users would now be used to provide that individual with information about current road blocks and to suggest alternative routes that would allow an escape.

A national strategy is needed

In the example of self-driving cars, a scenario emerges where whoever controls the database has access to more up-to-date and detailed information than the municipalities and authorities. Geographic data will also be gathered for various other purposes and stored in databases in other countries. Who will own the rights to this data? Will a private consortium of car manufacturers be able to sell and distribute information about Swedish infrastructure to anyone willing to pay? Would this mean that we have no idea who has access to up-to-date, detailed geographic information about our own territory? What degree of control would we have over this kind of data? Today, mobile phone operators are obliged to provide communications-related information in investigations of serious crimes. Issues regarding the legislation and regulatory framework concerning geographic data should be examined in a similar way.

The pace of developments raises a number of complicated questions that need answers. Geographic information is a vital and rapidly changing asset. A new strategy will be an important part of building a free and open, but safe and secure society.

11. The Long-range Weapon Threat

Erik Berglund, Martin Hagström and Anders Lennartson

Long-range weapons for use against targets on the ground, in the air or at sea have been gaining a great deal of attention on the world stage, most notably the Russian and US cruise missile strikes against targets in Syria, the North Korean missile tests and the deployment of US missile defence to South Korea. Long-range weapons have the potential to radically alter national security, but their impact has to some extent been exaggerated. There is a tendency to assess long-range weapons just by looking at their nominal range from a geographical point of view, but this is not always a valid assessment of their effectiveness – especially against moving or mobile targets. Security and defence policy has to be founded on realistic assessments of threats and capabilities. Accurate threat analyses based on technical facts are therefore of vital importance.

Long-range weapons can provide both tactical and strategic advantages in a conflict. They allow a threat to be projected while out of range of an opponent's weapons. In addition, the opponent will need to implement various tactical and technical means of protection. The term long-range weapon often refers to missiles. Missiles can be launched from the ground, the air or the sea against fixed or mobile targets. Missiles are classified according to their construction, their launch platform and their intended targets. Cruise missiles and ballistic missiles are used against targets on the ground. Ballistic missiles are propelled at high speeds and high altitudes, from where they fall towards the target in a ballistic trajectory. Ballistic missiles have traditionally been designed for far away targets on the ground, often on other continents. A cruise missile flies much slower than a ballistic missile and often at low altitudes. A cruise missile is propelled by an engine throughout its flight and navigates to reach its target.

Anti-ship missiles and surface-to-air missiles (SAMs) are examples of missiles for use against moving targets. To be able to hit a moving target, the missile needs a seeker, some sort of sensor that can be used to steer the missile to the target. Anti-ship missiles are basically cruise missiles fitted with a seeker that can detect ships. Surface-to-air missiles are launched from the ground or from vessels against aerial targets such as aircraft or missiles.

In the past decade, long-range missiles have become increasingly common in the Swedish neighbourhood. Russia has deployed the *Iskander* surface-to-surface missile and the *S-400* surface-to-air missile in the Baltic Sea region. In addition, the *Kalibr* cruise missile has been deployed on ships in the Baltic Sea. Finland and Poland recently acquired long-range weapons in the form of the stealthy cruise missile *JASSM*, while Germany has had the *Taurus KEPD 350* cruise missile for more than a decade. Sweden is currently upgrading its anti-ship missile inventory.

There is also intense activity in other parts of the world. Both Russia and the United States have used cruise missiles against targets in Syria while in North Korea there has been a steady stream of more or less successful launches of increasingly advanced ballistic missiles.

Realistic threats against moving targets

There are fundamental differences in the threat long-range missiles pose to fixed and moving targets. A moving target that follows a dynamic trajectory must be continuously tracked. Mobility therefore constitutes a form of protection and the target enjoys an advantage. For stationary targets, however, modern technology has shifted the balance in favour of the attacking cruise or ballistic missiles.

One long-range weapon that has attracted considerable attention in Sweden is Russia's S-400 SAM system. Its nominal range of 400 km means that the S-400 could theoretically reach Swedish territory. However, the actual range of a SAM is limited by a number of factors. An obvious factor is the curvature of the earth. Figure 11.1 shows that at a distance of 400 km, an aircraft needs to be at an altitude of 12 000 metres to be visible from the ground. Conversely, an observer needs to be at an altitude of 12 000 meters to be able to detect an object on the ground from this distance.

Another limiting factor is the flight time of the SAM. It takes about ten minutes for a SAM to travel 400 km, which is enough time for a fighter aircraft to fly more than 100 km in any direction. Consequently, a long-range SAM would need to receive real-time updates of the target's position and velocity in order to adjust its trajectory. This would require airborne or surface-based sensors to track the target and transmit data to the missile via a data link. All of this requires line of sight between the target and the sensors, as well as between the data-link transmitters and the missile. Terrain masking poses an obvious challenge for detecting and tracking targets at low altitude.

Furthermore, the missile has a limited supply of velocity, which would be quickly drained as the target manoeuvres.

All of this means that while a long-range SAM system such as the S-400 would certainly be a threat at a very long range to an airliner cruising at 36 000 feet, the actual effective range against a fighter at low altitude could well be under 20 km, depending on the terrain.

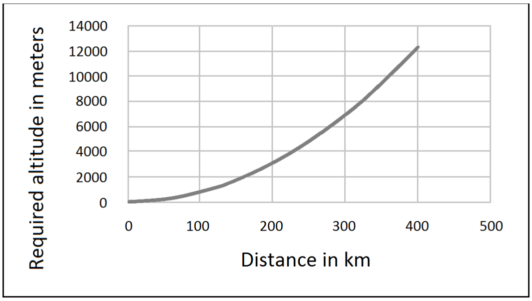


Figure 1. Required altitude for visibility of objects at a distance.

Hence, long-range SAMs constitute only a limited and to some extent manageable threat to fighter aircraft. For a SAM system to reach its full potential, it needs to be an integrated part of a network of sensors, command and control functions, and weapons. To be effective at long range, airborne sensors are required. Thus, the threat posed by a long-range SAM system in Kaliningrad or on Gotland, for example, cannot be described as a circle on the map with the nominal range as the radius. An aircraft taking off from an airbase in Sweden could not be shot down by SAMs based on the other side of the Baltic shortly after it left the runway.

Attacking moving targets at long range requires a chain of sensors, command and control, weapon platforms and weapons that is both accurate and fast. The United States is probably the only country that currently has the capacity to use long-range weapons against mobile ground targets or time-critical targets.

Severe threat to stationary objects

Because the target's position is known in advance, long-range attacks can be made against stationary targets without any sophisticated system of sensors. Consequently, cruise missiles and ballistic missiles are highly realistic threats to stationary objects and need to be taken into account by Swedish defence planning.

As long as the position of a target has been identified with a high degree of accuracy prior to the attack, a cruise missile or ballistic missile strike can be made with a high level of precision. Fixed targets such as buildings, runways or parts of the power grid can be targeted well in advance, based on satellite imagery.
The ballistic missiles that pose a potential threat to Sweden are primarily those based in Russia. The *Iskander* has a range that most sources put at 400–500 km, which means that it could reach parts of Sweden. Furthermore, the *Iskander* has a short flight of less than 10 minutes from the other side of the Baltic – and a high level of precision. The *Iskander* cannot be used against moving targets, but its short flight time means that it could be used against targets of a temporary nature such as command and control sites or forward arming and refuelling sites.

Trends

The development of high-tech long-range weapons is likely to continue at pace. Developments in guidance and navigation coupled with a general proliferation of technology will make long-range cruise missiles increasingly available and affordable. Cruise missiles, which used to be the trademark of a superpower, are about to become available to many countries or even non-state actors, and possibly also to individual terrorists.

There is a trend among the advanced countries for cooperative engagement based on networking sensors, command and control functions, weapon platforms and weapons. Such cooperation aims to quickly establish situational awareness when carrying out a mission. The purpose is to provide missiles with real-time target data to enable the target to be hit in a coordinated salvo. For long-range cooperative engagement to work, high-performance sensors and secure datalinks are of paramount importance. The United States is leading in the development of cooperative engagement, especially for strikes against ground targets.

High-speed missiles are another trend. High-speed in this context means speeds in excess of 3000 km/h. This reduces a missile's flight time, which gives the intended target less time to react by manoeuvring, deploying countermeasures or returning fire. High speeds are also important to reduce a missile's vulnerability to air defences, for example when an anti-ship missile is attacking a combat ship. The Russian-Indian *BRAHMOS* anti-ship missile can reach speeds of about 3000 km/h and the *BRAHMOS II* is being designed to reach 5000 km/h.

Countermeasures against long-range missiles

During the Cold War, the main threats to fixed objects were enemy bomber aircraft and sabotage by special forces. The identity and location of many installations could be concealed using physical perimeters, camouflage and the control of information. Enemy bombers would have to get close to their targets, which would expose them to air defences. Today, however, the ability to conceal the location of installations is much more limited. High-resolution satellite or aerial imagery is currently available even to actors that lack their own reconnaissance systems.

Ground-based air defences can be effective against both cruise missiles and ballistic missiles. However, there is a striking imbalance in the fact that many defensive SAMs are more expensive than the offensive cruise missiles they are defending against. Furthermore, the defended area is small, as cruise missiles can exploit the terrain to avoid detection and the high velocity of ballistic missiles limits the effective range of SAMs. In reality, this means that the area that can be protected by an advanced ground-based air defence system with a nominal long range corresponds to a single airbase or a medium-sized city. Advanced sensors, in particular air-borne sensors, integrated with the SAM system can significantly increase the area that can be protected, but such sensor systems come at a high cost.

Thus, technology has given an advantage to the attacking side, at least for stationary ground-based targets, and there is an imbalance between threats and protective measures. An illustration of this is Israel's recent launch of two Patriot missiles, which cost around US$ 3 million each, to shoot down a drone over Syria. If inexpensive drones and cruise missiles proliferate to an increasing number of actors, including non-state actors, the cost of using advanced air defence systems as protection will become unattainable.

One way to defend against long-range weapons is to strike first to prevent their launch. This requires your own long-range weapons and very good intelligence about the location of enemy assets, especially if the enemy is using mobile launchers. A method that works against the cheaper weapons employed by non-state actors is to jam satellite navigation systems in the vicinity of the target. In addition, traditional methods of protection such as underground fortifications, decoys and camouflage remain highly relevant.

Moving or mobile targets still represent a challenge for long-range weapons. Attacking a moving target requires a fully functioning chain of sensors to provide target data, command and control functions and the right weapons, all of which can be vulnerable to both weapons and electronic warfare.

Correct technical analysis is essential for the right type of protection

Long-range weapons are very powerful and play an increasingly important role in battle. Technological developments have given long-range missiles, including ballistic missiles, a high degree of accuracy. However, against moving targets the difference between the nominal effect of a long-range weapon and its actual effect is highly significant.

Protective measures and countermeasures will differ for stationary and moving targets. As most types of countermeasure and protection are extremely expensive, it is of paramount importance to analyse the threat against each type of target and to find the most appropriate way to protect against them. Taking measures to protect against a threat that has been overestimated can be just as costly as underestimating a threat and neglecting to take countermeasures.

12. Sweden Needs a Defence- and Security-related Space Strategy

Sandra Lindström och John Rydqvist

In some respects, Sweden is an advanced space nation. Investment in military space systems, however, is still modest, and civilian and commercial interests are the primary propellants of Swedish space-related research and engagement in the space domain. This is reflected in the proposal for a Swedish space strategy that emerged from the 2015 Space Inquiry. Dependence on space-based services increases in parallel with greater use. This is true also in the military sector, where dependence on space-based systems is becoming increasingly evident. There is a risk that if Swedish space policy does not pay more attention to and put more emphasis on the defence and security policy aspects of space-related activities, Sweden will be left behind by a range of other actors. In addition, the development of future space-based services and the ability to handle likely threats and risks might be hampered in ways that in the long term could have implications for national security.

The importance of space in a deteriorating security situation

Sweden's security situation has deteriorated since 2008. As a small state with an interest in protecting and promoting the norms and agreements on which the prevailing international system is based, Sweden has adopted numerous measures to increase common security. EU membership and the solidarity nominally associated with it is an important dimension but important security policy partnerships have also been developed with the USA, Finland, Norway and NATO. Measures to strengthen the possibility of joint action in the event of a crisis or war are being complemented by enhanced capabilities as well as better coordination, situational awareness and information-sharing, and secure infrastructure for the Swedish concept of total defence.

Since the 1960s, space-based systems and services have been important in many states for strengthening their capabilities to pre-empt risks and threats, and increasing their capacity to defend themselves. Today, many states rely on satellite navigation services, space-based Intelligence, Surveillance and Reconnaissance (ISR) and satellite communication, for both civilian and military uses. In several instances, the same system is used by both sectors, and space is one of the arenas where this type of dual use is most apparent. Technical and conceptual developments in the space domain are advancing quickly. The future role of space-based systems is therefore seen as of ever-increasing importance to defence and security.

Sweden has been slow to make the connection between the security architecture in space, and defence and security policy. Swedish space-related activities have primarily been an academic and industrial issue, which has meant that the development of civilian space activities has dominated. At the same time, however, Sweden uses space-based services in its defence and security sectors on a daily basis. This usage is likely to grow as the range of available services increases and their quality improves. To date, military developments in space have involved various parallel activities linked to short-term operational requirements, and have not been the result of a long-term overarching strategy.

Space trends and future space threats

As a result of the global development of the space domain, Sweden, too, has become more productive and efficient. For example, satellite communication can be used to broadcast crisis information during major accidents, when cellular networks have broken down or become overloaded. Satellite navigation saves money when building highways and contributes to more fuel-efficient freight traffic. For stock markets, banks and trading firms, the exact timekeeping delivered by GPS satellites is vital for conducting their operations. These advancements also exemplify dependencies that space-based services have created in civil society. These dependencies, in turn, also lead to a number of defence and security related threats and risks that Sweden must be able to deal with. Three overarching space-related threats or risks have been identified internationally:

First, many states are increasing their military capabilities with the aid of satellite services, not only through their own systems, but also using the growing network of commercial services. There are also examples of non-state actors, such as rebel or terrorist groups, making use of space-based services. Access to space has been ensured through several independent national launch programmes, a technology that can also be used to develop ballistic missiles. Both Iran and North Korea currently have a launch capability. Pakistan and Turkey have ongoing development programmes.

Second, military logic leads to the development of concepts and plans to prevent a potential enemy from gaining access to space-based services in the event of a conflict. This is a consequence of the ways in which space systems have become crucial for dealing with broad questions of national security and for the conduct of war in several major powers. If space-based systems and services are a prerequisite for conducting operations, the need to secure and protect those systems follows. There will also be a drive to limit access by potential opponents. Consequently, leading space nations such as the USA, Russia and China have continued to develop anti-satellite technology.

Third, near Earth space has become dramatically more congested and littered with debris in recent decades as a result of the more frequent use of space by more actors. This increases the risk of collisions between satellites. The most pressing problem, however, is space debris, or uncontrollable objects of varying sizes that have been left or lost in orbit. There is currently no efficient way to collect these objects. Nor is there any consensus internationally about how the problem should be dealt with. This is a long-term problem as many objects can remain in orbit for decades or even centuries before they descend and disappear. In certain scenarios, the amount of debris increases exponentially as a result of sequential collisions, in the end rendering space unusable. The same effect might be the outcome of a deliberate attack on a satellite.

A limited Swedish space strategy

Even if Sweden has become more productive and efficient due to its ever-wider use of space-related services, there is still enormous potential for improvement that would allow Swedish space-based activities to become even stronger and more competitive. The need for a cohesive strategy on the development of the space sector has therefore received attention in recent years. The resulting government Commission of Inquiry published its report, *En rymdstrategi för nytta och tillväxt* (A space strategy for benefit and growth), in 2015. The report concentrated primarily on civilian and commercial interests, and envisaged ways in which Swedish space research and related activities can continue to contribute to growth and increased employment. This approach reflects the traditional approach to space-related activities in Sweden, with its focus on civilian and academic research and development.

The defence and security policy issues discussed above make the direction of the strategy proposed in the report problematic. It certainly raises the need for better civil-military coordination, but it lacks a defence and security perspective more generally. For a document that is intended to be the foundation for a national space strategy, this is a serious flaw. This begs a number of questions:

- Is there sufficient understanding of the security implications of current and future space systems, and has Sweden's use of space been thoroughly thought through?
- Are there sufficient knowledge, the right capacity and the coordination needed to assess adversaries and meet eventual threats?
- How can the accumulated knowledge and experience of the civilian sector be used when the importance of space to defence and security policy becomes more tangible?
- What are the risks if the defence and security policy perspective fails to have an impact on national space strategy?

Space activities are generally undertaken in the civilian, the commercial, the military and the intelligence sectors. The national space strategy should be able to connect these four sectors more clearly than was the case in the Inquiry's proposal. It must set out how Sweden can retain and develop the strengths of its current space activities; and make proposals on how defence and security policy aspects can be more thoroughly considered, as a complement to and a strengthener of the industrial and academic aspects. It should be possible for the space strategy to identify in a more visionary way the long-term opportunities available to the defence and security sector, given the rapid development of the space domain.

The space-related opportunities for Swedish defence and security

In some areas, Sweden is an advanced space nation. International trends in the space arena correspond in part with what is happening here at home. However, there appears to be several opportunities for Sweden to make new and additional national advancements. For example, the development of small satellites, coupled with cheaper launch alternatives, could provide future opportunities for Sweden to build, launch, operate and use its own national satellites free of the oversight and restrictions of other states. Other areas that could be further developed and strengthened are useful not just for the civilian and commercial sector, but especially for the military and even the intelligence sectors:

- propellants for ballistic missiles and space rockets
- space-based situational awareness
- robustness-enhancing technology for satellite communications as well as space-based positioning, navigation and time synchronisation (PNT)
- space-related electronic warfare
- ISR from space.

There are many opportunities to develop national capability domestically, as much in research and technology development as operational capability. For example, academic research could be commissioned on the problems associated with space debris. The satellites launched by the Swedish state could also be seamlessly employable in defence and security research as opportunities arise.

Expanded knowledge of how both Sweden and the rest of the world use and develop space services for defence- and security-related purposes increases the ability to assess an adversary's capability, but also plays a vital part in attaching a higher priority to Swedish development of space products and services. National capacities for research and technology development as well as operational services could be further developed, for example, to more clearly highlight the dual-use perspective. A broader Swedish understanding and acceptance of the space domain's many and complementary applications could also prepare the way for deeper and more extensive international cooperation in the defence and security field. It is likely that strengthened military engagement in space will also lead to more opportunities for cooperation with the already strong Swedish space industry and academe.

The need to formulate a more complete Swedish space strategy

According to the space inquiry report, military space-related activities make up less than 5 per cent of the state's total commitment to space activities. Such military activity, however, is an emerging sector and the significance of the space arena for Sweden's defence and security is steadily growing. According to a 2016 report by the non-profit organisation, the Space Foundation, the USA invests approximately 53 per cent of its national space budget on defence and security, while the rest of the nations of the world together invest an estimated 33 per cent of their national budgets on defence and security. Any new

Swedish space strategy should ensure that all four sectors – the civilian, commercial, military and intelligence sectors – are pursued in a balanced way. It should be possible, for example, to devote more attention to the synergies between civilian and military interests. Current research and high-tech product development needs should also be identified and development started to ensure that defence and security needs are met in the long term. The strategic direction should be set so that Swedish space-related activities help to enhance military capabilities and strengthen Swedish defence, thereby providing a more secure Sweden. This can be achieved by building on existing strengths and identifying development opportunities.

The proposed national space strategy must therefore be complemented with a dedicated defence strategy for space. This could either be a freestanding document or integrated into the comprehensive national strategy. A defence and security strategy for space would discuss all the operational authorities' needs, materiel supply, regulations and permissions, export questions and educational requirements, as well as research and technology development. It should consider current strengths and weaknesses, and future opportunities and threats in relation to space-based activities. All the relevant total defence entities should be included and given clear roles.

The absence of a Swedish defence and security strategy for space issues has prevented effective utilisation of space-based services for national security purposes. Sweden currently relies on commercially available space services or international cooperation in the defence and security sector. Dependence on other states leaves Sweden vulnerable. Failure to tackle these issues in a clear way risks leaving Sweden ill-prepared for the future. This is as much about taking advantage of development opportunities as the threats and risks that the Swedish state might face as other actors advance their positions and strengthen their capabilities in the space domain.

A strategic outlook for the future

Sweden has long been a space actor and Swedish society has a high level of dependency on a wide array of space systems and services, both civilian and military. Our dependence on, for example, the US GPS system is such that it will not be either economically or practically possible, even in the medium to long term, to move towards relying exclusively on the EU's satellite navigation system, GALILEO – a system that Sweden has been part of setting the parameters for and helped to finance by virtue of its membership of the EU. The absence of a long-term, comprehensive national space strategy is probably a strong contributory factor to why we find ourselves in this situation.

In the rest of the world, the space domain is developing rapidly. The number of new actors with satellites in space has almost doubled since 2000. Even less technically advanced developing countries are establishing their own satellite systems, since the technology is now so accessible and becoming cheaper. This is also a way for these states, in parallel and in cooperation with other states, to develop their own domestic research and industry, and to strengthen their defences. Dependence on space-based services means that these assets have to be protected. The development of anti-satellite programmes by the major space powers is especially worrying. At worst, it could see space becoming the new arena of conflict.

It is right that the proposal for a cohesive Swedish space strategy highlights the need for increased civilian-military collaboration. The problem with the proposal is that it fails to offer suggestions on how such collaboration could be achieved. Instead, the proposal reflects how Sweden has traditionally pursued its space-related activities. Questions or activities that could directly enhance or contribute to national defence and societal security are hardly mentioned at all.

Sweden is a small country with limited resources. It is unrealistic to believe that it will ever be possible to undertake broad and comprehensive civilian and military space-related activities and space-based development alone. Nonetheless, Sweden must continue to develop its utilisation of space in all sectors. A first step in finding a balance will be to produce a defence and security strategy for space issues that, together with the civilian strategy, would set national priorities for and make fundamental decisions on the future of Swedish space research and space-related activity.

13. Sweden’s Food Supply after Radioactive Fallout: Five Loaves and an Entire Population

Niklas Brännström, Torbjörn Nylén and Henrik Ramebäck

Sweden has lost parts of its capability to deal with crises where radioactive fallout is an issue. In a situation involving the unthinkable, where Sweden is attacked with tactical nuclear weapons, this would be brought to a head and place major strains on all parts of society. An attack with tactical nuclear weapons, apart from direct destruction and damage, would have major consequences for Sweden’s food supply. The ability to predict where fallout settles, measure the activity of radionuclide deposits, determine uptake into food and calculate the radiation dose that would result from consuming the contaminated food must be strengthened. Decision-makers must dare to consider this scenario and once this thought has been thought, ask themselves what form of decision support they would need in order to act. The capacity to deal with such a scenario needs to be assured through appropriate measures, training and exercises.

A trade-dependent food supply

Sweden imports approximately half of all the food that is consumed in the country. This applies to most of the fruit and vegetables and more than half of all meat. For certain products, such as tea and coffee, it relies entirely on imports. On the other hand, the proportion of dairy products and grain that is imported is small. If the pattern of trade with other countries changes, this affects the selection available in grocery stores. This was noticeable during the cold snap that affected the Mediterranean in the winter of 2016. Suddenly, certain vegetables were missing from the produce section and the price of many of those still available increased substantially.

Fruit and vegetables are special in that respect, since many have a short shelf life and cannot be stored if supply is suddenly reduced. For many other foodstuffs, stockpiling can resolve a temporary shortfall in production or imports. During the Cold War, Sweden’s agricultural policy made us almost completely self-reliant in food. There were also stocks of food, as part of crisis preparedness. In the early 1990s, however, agricultural policy was reformed to make it market-driven, and the last food stocks were dismantled at the beginning of the 2000s.

Storage is expensive for both states and shop owners. It is more efficient and profitable to sell an item immediately after it is delivered to the store. The problem is that this gives rise to vulnerability; when deliveries cease, the food disappears. If, however, neither the nation nor the grocery store has any stocks that can cover a short-term disruption: who should have? In the spring of 2017, the Swedish Civil Contingencies Agency (MSB) working with the County Administrative Boards and the municipalities conducted an information campaign to increase Sweden's crisis preparedness. One message, for example, was that all citizens were encouraged to maintain their own supplies – a 'crisis box' to help them manage during a brief interruption in food imports.

Notwithstanding the seriousness of cold spells or transport strikes, there are also more serious threats. What would be the effect, for example, of a war in Sweden's neighbourhood combined with radioactive fallout over Swedish agriculture? How long would citizens' stocks of food last in such a situation? What could be done before clean-up measures and a reorganisation of production restored domestic food supplies?

A worsened security situation

The security situation in Sweden's neighbourhood has deteriorated and the conflicts in Georgia and Ukraine demonstrate that the threshold for armed violence has been lowered. To the image of a generally worsening security situation should be added the fact that the USA and Russia are continuing to develop the capabilities of their nuclear weapon systems. France and the UK have also committed major resources to maintaining their nuclear capabilities. Even had the Comprehensive Nuclear Test-ban Treaty fully entered into force, there is no agreement that forbids the use of nuclear weapons to achieve tactical or strategic goals in an armed conflict. The use of nuclear weapons is part of Russia's defence doctrine as both a tactical and a strategic tool. Russia regularly conducts exercises with its nuclear weapons units and it is reasonable to assume that a rational nuclear-weapon state would consider the use of nuclear weapons if the situation required it. An attack using tactical nuclear weapons in a regional or local conflict is a genuine threat. This has been pointed out in the joint understanding between the armed forces and the MSB on cohesive planning for total defence.[8] The military-strategic doctrine of 2016 also discusses the threat from tactical nuclear weapons and concludes that our defence

[8] *Sverige kommer möta utmaningarna* [Sweden is going to meet the challenges], FM2016-13584:3/MSB2016-25.

must be prepared for such a threat. It is therefore important that such situations are dealt with within the framework of crisis and defence planning.

If the unthinkable were to happen

Let us consider a situation in which a limited attack using remote weapon systems against military targets, including its logistics functions, took place in Sweden. The fortunes of Sweden's enemy have quickly turned and as a result it feels under pressure to guarantee the outcome of the attack. Thus, in addition to conventional weapons, a small number of tactical nuclear warheads are detonated against these targets. Apart from the initial radiation, and the shock and heatwaves as well as the ensuing firestorms, a large amount of soil is thrown into the air and radioactive particles of varying sizes are formed. Depending on the size of the particles, some will fall to the ground close to the site of the detonation, while others will be transported on the wind. Certain particles will be thrown high into the atmosphere and spend decades there before falling back to earth.

An attack of this kind would plunge Sweden into the following crisis:

- Food imports would almost entirely cease because of the conflict and its impact on logistics;
- Locally, people will have received serious injuries due to the immediate effects of the nuclear detonation. Caring for them will consume a significant part of society's resources;
- Large segments of the rest of the population will have managed to find provisional shelter in a cellar, bunker or similar; some of these will have complied with the MSB's appeal to maintain a supply of food at home. They will therefore be equipped to survive the first few days;
- Domestic transport of foodstuffs and other supplies will be hampered by a shortage of transport and fuel, as well as by damaged infrastructure. Radiation levels in the affected areas are also likely to create problems. Not even the threat of impending starvation will bring all agricultural land back into production. Near the detonation site, radiation doses will be so high that it will not be possible to stay there. Farmers will not be able to work in their fields.

One uses what one has

To continue the scenario, storage shelves will be emptied and that part of the population that has not complied with the MSB's request, or that does not habitually keep dry foodstuffs in the pantry, will go hungry. Soon the entire population will face a situation of hunger. Domestic food production will be affected by radioactive fallout to varying degrees and there will be many questions: What proportion of agriculture survived the attack? Is it possible to use the affected land? Is the fodder fit for livestock to consume? Can the grain and meat be eaten? Is the milk drinkable?

Because, for logistical reasons, a sizable percentage of imports have been cut off, after some time only Swedish commodities will be available in the shops. A proportion of these will not even be "second-class fresh", to quote Michail Bulgakov's classic description of the quality of foodstuffs in post-war Moscow in *The Master and Margarita*. The crops that grow in the fields (if they grow) will be so contaminated that they will not be marketable or suitable as fodder, according to the limits that the EU contemplates imposing after radioactive fallout. On the other hand, they may be edible under the threat of starvation. In addition, it might be possible to clean the harvested commodities of surface contamination and keep them in storage while waiting for the decay of radioactive substances with short half-lives.

Difficult choices require good decision support

In this situation, decision-makers must decide what level of radiation dose it is acceptable from the ingestion of food. Sweden has a certain level of preparedness for radiation protection and radiation medicine in the event of a nuclear reactor accident, as well as a certain capacity for mapping fallout and measuring radiation doses in humans, and performing laboratory measurements on samples from pasture, commodities and food. This capacity is in all probability not sufficient for dealing with a nuclear weapons scenario, which requires data in the form of contamination measurements and radiation dose calculations, as well as medical examinations to set priorities for medical treatment. Even the capacity for measuring whether the contamination of food is within established limits or clearance levels would be inadequate in a situation where examining affected people will be prioritized higher than measuring foodstuffs.

There is currently no national plan for rapidly organising sufficiently large capacity for measuring radioactive substances in food. Peacetime responsibility for demonstrating that a foodstuff is within EU safety limits lies with those who distribute or sell the product. It is safe to assume that if there are difficulties in importing food during a crisis, then other imports such as of instruments for carrying out radionuclide measurements would also be affected. Constructing new certified measurement laboratories and providing the personnel and measuring equipment capable of handling fundamental metrological quality criteria would be no simple task. High metrological quality will be essential if decision-makers – and in the end the population – are to depend on the measurements to form the basis for decision making on whether land can no longer be deemed dangerous.

The absence of a national plan will probably mean that the few resources that are available will be used for spot checks on food, commodities and land. The primary aim would be to validate predictions on levels of contamination in commodities and food, and calculate the resulting internal radiation dose for the population. These predictions would be based on the meteorological conditions at the time of the detonations and knowledge of how plants capture and retain radioactive substances in their tissues. It is exactly these theoretical models that are likely to provide decision-makers with the most complete basis for planning countermeasures and measurement operations, but they are only partially available nationally. In addition, because the nuclear weapon threat has long been assessed as low, methodologies have not been devised to function in this kind of scenario.

The limited capacity to either predict or actually determine the radiation dose obtainable from food after a nuclear attack will lead to difficulties in judging the safety of foodstuffs. Unsafe contaminated food will probably be consumed while edible foods are discarded by mistake. The authorities will have a difficult task making decisions on temporary clearance levels that will be much higher than the consumer has previous experience of. It is important that society has a mental preparedness for a situation such as this. It will also be crucial to find ways to deal with such a situation, to establish resource and quality standards for conducting national measurements and to develop forecasting tools and principles for making decisions. We must be able to weigh the respective consequences of malnutrition and hunger or high radiation doses from food against each other. It is reasonable to expect that the results of such considerations should be on the table well before a situation involving radioactive fallout might arise.

Five loaves and an entire population

Even if society were to decide to allocate the means to build a capability to operationally assist with the types of tangible capabilities that enable good decision support, many challenges would remain. Planning tools must be improved, in part because of the risks that could arise and the need to communicate them to the population in a credible manner, and in part to ensure a sufficient metrological capacity as well as priorities for food distribution. If this fails, there is a great risk that everything, from food shortages to starvation, will lead to a loss of confidence in the authorities and other decision-makers. At worst, this would lead to mass migration from the city to the countryside, and to tensions between those who have and those who do not.

Further Reading

S. Holmgrem, A. Tovedal, O. Björnham and H. Ramebäck, "Time optimization of ^{90}Sr measurements: Sequential measurement of multiple samples during ingrowth of 90Y", *Applied Radiation and Isotopes*, 110 (2016), pp. 150–154.

P. von Schoenberg, P. Boson, H. Grahn, T. Nylén, H. Ramebäck and L. Thaning, "Atmospheric dispersion of radioactive material from the Fukushima Daiichi nuclear power plant", in Steyn et al. (eds), *Air Pollution Modeling and its Application XXII* (Springer: Dordrecht, 2014).

14. A Norwegian Outlook

Alf Christian Hennum and Tore Nyhamar (Norwegian Defence Research Establishment, FFI)

NATO is an essential instrument in the defence of Norwegian territory. Norwegian defence planning therefore takes as its point of departure the need to ensure assistance from NATO in the event of a military attack. To enable such guarantees, Norwegian defence planning must balance Norway's national needs with those of NATO. Norway therefore tailors its defence capabilities in such a way that will assist NATO and defend its own territory. Any strategic defence prioritization, from the acquisition of material systems to the stationing of Norwegian armed forces, should be seen in this light.

The Alpha of Norwegian Defence Policy

The main task of the Norwegian Armed Forces is to secure Norwegian sovereignty and political freedom of action. Since Norway signed the North Atlantic Treaty in 1949, NATO has been the cornerstone of Norwegian defence and security policy. Throughout the Cold War, Norway's strategy as a small state was premised on the availability of NATO military reinforcements, and that remains the case today. NATO has developed since the end of the Cold War. The increase in the number of member states, combined with a threat that many members now perceive as more about political influence than resisting conquest, has led to an increase in the range of strategic perspectives and priorities within the Alliance. Consequently, the number of situations that are unambiguously guaranteed to trigger article 5 has been reduced. NATO has gradually changed in character from a traditional defence alliance to a consultative security organization with a military capability. Exactly where it is located on that spectrum is contested and will vary according to circumstances. For the purposes of this chapter, the point is that current Norwegian defence planning must include as an important element a strategy aimed at securing NATO help should Norway face a situation that is too demanding for its national forces.

After the Cold War, NATO prioritized expeditionary operations ("out of area or out of business"). Norway participated in these operations, most notably in Afghanistan, to help to ensure the continued relevance of NATO. Unlike Denmark, however, Norway never abandoned the defence of its own territory as the primary task of the Norwegian Armed Forces. NATO's refocus on the territories of its members ("coming home") after 2014 was therefore a welcome development, especially as it was triggered in response to a more capable and assertive Russia. The threat Norway now faces has also evolved from the existential threat that was posed by the Soviet Union. Today, Russia is perceived as the only country with the capability and, potentially, the will to use armed force against Norway. Russia's capability, however, is significantly smaller than that of the Soviet Union. In addition, if a conflict were to take place between the two nations, Russia's objective would be political influence rather than the territorial conquest that was its aim during the Cold War and that Norway's defence planning was then intended to avert. Thus, the challenges to Norwegian security would appear to have two sources: military force being used against Norway or Norwegian interests in a locally rooted bilateral conflict; or military force being used in a horizontal escalation of a conflict originating outside Norway.

The Importance of Deterrence

The concept of deterrence is currently central to defence planning. The concept was explicitly used in official government documents only recently, but has its roots in deterrence theory from at least as far back as the 1960s (deterrence by punishment), and has implicitly been part of Norwegian thinking about defence since then. Today, when threats and guarantees are perceived as fuzzier, the concept is subject to explicit discussion. Deterrence belongs partly in the cognitive domain and partly in the physical domain. In the cognitive domain, the objective is to impress on potential aggressors that pressure or an attack on Norway will not pay off. In the physical domain, the task is to have sufficient military means, and the up-to-date and sufficiently exercised plans to employ them effectively, should deterrence fail. Exercises such as Trident Juncture 18 have contributed in this respect. NATO is the most important deterrent against a military attack on Norway. Norwegian deterrence has therefore recently involved measures to ensure that the Norwegian Armed Forces operate in ways that would unambiguously trigger military reinforcement from NATO.

The most important defence measures for Norwegian security are thus to have the national military means that can help *trigger* assistance from NATO, as well as have the ability to *secure* and *receive* those reinforcements. Force structures and defence concepts are part of this, as well as weapon systems, and up-to-date plans for how help would be received. Finally, Norwegian defence planning also prioritizes contributions to enhance NATO's ability and willingness to act. For example, Norway must have the military forces to contribute to NATO's rapid reaction forces, such as the NATO Response Force and its standing maritime and air forces.

Norwegian Long-term Defence Planning

A major challenge for long-term defence planning since the end of the Cold War has been to establish a clear link between security challenges and political ambitions, on the one hand, and recommended force structures, on the other. What specifically should Norway's forces be able to do and which platforms and units are needed to do it?

A main element of Norwegian defence planning has been the Defence Studies initiated by the Chief of Defence (CHoD). The methodological approaches of these studies have varied, but together they have been the main driver of a demanding but necessary transformation of Norwegian defence.

Since 2014, the defence planning process in the Ministry of Defence (MoD) has been continuous. This has meant that the necessary analyses can be conducted and decisions taken in the periods between traditional defence white papers, which are produced every four years. Prior to the writing of a white paper, the CHoD presents military advice (*fagmilitære råd* or FMR) on how the Norwegian armed forces should develop. The FMR has traditionally had a great impact on the political white paper and often sets the stage for the political debate. However, the FMR is only CHoD advice to the minister. The MoD itself is responsible for the formulation of the white paper, which is then approved or amended by parliament. A *strategic analysis* is conducted as part of the writing of the white paper. The method is in principle based on capabilities and uses high-level capabilities to structure the analysis. The most recent white paper, *Capable and Sustainable*, emphasised the need to balance tasks, force structure and costs. The top priorities were to strengthen Norwegian national defence by:

- maintaining situational awareness and crisis management;
- increasing readiness, combat power and survivability;
- improving the ability to receive NATO reinforcements;
- increasing the military presence; and
- more frequent exercises and training.

The decision to improve the capability to receive NATO reinforcements matters greatly because the Norwegian host nation support system had fallen into disuse and not been updated since the end of the Cold War. The host nation systems are still in place, but the plans and procedures need to be adjusted to the changed realities of the 2020s.

In the research phase of the defence planning process, the analysis effort is focused on the fighting units and how these should be developed. There are good reasons for this: the fighting units are the ones that perform the defence tasks and an analysis of these units is somewhat simpler to conduct than analyses of support units and infrastructure. The purpose or mission of the fighting units is usually clear and levels of ambition can be clearly stated. Support units, on the other hand, often have complex relationships with other defence elements, and the impact of changing these units is therefore more difficult to assess.

Norwegian long-term defence planning has struggled with the cost escalation specifically associated with military materiel. Traditionally, this has not been taken into account when new budgets are negotiated. The result is a force structure that is too large compared to its funding and that fails to produce the military fighting power expected. The difficulties in analysing the ratio between fighting and support units compound the problem. This problem, which is not unique to Norway, has finally been addressed in the most recent white paper. If paper is implemented, the result should be a force structure that is properly funded and sustainable over time.

Prioritising between Norway's and NATO's needs

The long-term planning process has focused mainly on national requirements. The NATO defence planning process (NDPP) has received some attention, as it should, but Norwegian national scenarios and force structure legacy dominate the defence planning process. Dependence on NATO is neither forgotten nor neglected, but concern about NATO influences long-term defence planning in more ways than just the aim of closing NATO capability gaps. As one of the smaller NATO member states, Norway cannot make much of an impact on those gaps on its own.

Furthermore, Norway emphasises investment in defence capabilities that can contribute to NATO while remaining relevant to its own defence. A strategic priority is the strengthening of Norway's ground-based air defences. The medium-range Norwegian Advanced Surface-to-Air Missile II system (NASAMS II) will be upgraded and enhanced through the addition of missiles with an extended range. In addition, new air defence systems with long-range missiles and sensors will be introduced. Air defence is obviously a national capability for national needs, but the priority given to NATO is demonstrated in the planned deployment of the systems. Both NASAMS II and the new long-range systems will be concentrated around the two airbases at Ørland and Evenes, which are critical for Norway's own forces but also serve as potential staging area for NATO reinforcements. The acquisition of the F-35 Lightning and the planned acquisition of new submarines are further examples of capabilities that enable Norway to maintain a presence and, if necessary, to act on its own behalf as well as for NATO.

In the High North, Norway is the only NATO country to share a land and sea border with Russia. This makes Norway's territory vital for a surveillance, intelligence and defence presence in the Arctic. Norway's acquisition of new maritime patrol aircraft – five P-8 Poseidon aircraft to replace the aging P-3 Orion – is a prime example of a capability that serves the needs of NATO. The prioritisation of all these capabilities is an example of the efforts made to create a credible Norwegian defence posture by contributing situational awareness and intelligence to both Norway and NATO. While advanced capabilities such as these might be perceived as a threat by Russia, it is less problematic for Russia for these tasks – inherent to any sovereign state – to be undertaken by Norway rather than by NATO or the USA. Together, these capabilities give Norway the ability to undertake crisis management either alone or as part of NATO.

The legacy host nation support systems are still in place, but continuous training in them is needed and they need to be updated to respond to current threats, after the hiatus in which NATO's attention was on out-of-area operations. Therefore, Norway aims to host exercises with participation by relevant member states, focused on quick response and territorial defence. Today, when a more limited and political threat is being planned for, readiness and response times are prioritised for both Norway's own military forces and in NATO exercises. The increased activity of the US Marines Corps, which is training more or less continuously in Norway, is a prime example of the new emphasis on smaller but quicker NATO responses.

A balanced defence planning

Norwegian long-term defence planning must balance national and NATO needs. Contributing to NATO capabilities is one way to do this. More important, however, is the way in which

Norway's own capabilities are tailored to undertake tasks that will benefit NATO as a whole while also defending its own territory. The priority given to the High North should be viewed in this light. That said, Norway's strategic challenge remains that it is more demanding to operate military forces in the North, far away from its population centres. The Norwegian Armed Forces face a lesser challenge in operating in the rest of the country. Norwegian planning is not confined to defence structures. Appropriate funding for relevant NATO exercises and to update doctrines are also strategic priorities. Finally, the key priorities of national defence are geared to being able to receive NATO reinforcements and to operate with them.

15. The Finnish Defence Planning Problematique

Jyri Raitasalo (Finnish National Defence University)

Finland's defence policy guidelines and defence planning principles have been subject to change in the post-Cold War era, most notably due to the changing nature of the international security environment. However, it is noteworthy that in the European context, whereas most Western states have made fundamental changes to the way in which they conceptualize international security, defence planning and the use of military force over the past 25 years, Finnish defence planning has been characterized more by continuity than change. Understanding this continuity is important when analysing recent defence policy decisions by the Finnish Government. The most recent of these is formulated in the Government Defence Report to parliament in February 2017.

The Legacy

> "The termination of the Cold War and the altered picture of potential crises pose new questions for the defence of Finland. With the decline in the threat of a major war, its place has been taken by the existence of regional crises that are susceptible to escalation. With crises becoming more obviously internal matters for individual states or otherwise spatially restricted events, we are obliged to adjust the structure and deployment plans of our armed forces accordingly. All in all, the image of future warfare has substantially altered."
> *Statement by the Parliamentary Defence Committee to the Foreign Affairs Committee, 1997*

Defence planning is the sphere of politico-military activity that defines the military threats to national security and in so doing also defines the core military tasks that armed forces must be able to perform. Defence planning is thus a politically guided process that sets priorities and allocates resources for the maintenance, development and use of military forces.

Defence planning is deeply ingrained in the strategic culture of the actor in question. Different states with different historical experiences and varying geostrategic locations have diverse ways of conceptualizing the kinds of threats that they must be prepared to counter, who or what should be protected from these threats, and what military means are effective or acceptable for doing so. In other words, how actors conceptualize war – its character, probability and goals – influences how they organize their defence planning.

During the Cold War, the foundations of Finnish defence planning were associated with the political security paradigm of neutrality and associated attempts to avoid being part of the great-power confrontation. Maintaining a defence capability to protect the territorial integrity of the country against military threats – without directly naming potential aggressors – formed the bedrock of Finland's Cold War defence policy outlook and defence planning principles.

With the demise of the superpower confrontation and the bipolar international system in the early 1990s, states and international agencies found themselves in a situation where the old rules of the international system were being questioned and 'new' or 'altered' rules had to be devised. However, this rule-changing process was not a formal one. Instead, it was a conjoined process of agent-level and system-level practices where assessments were made regarding the ending of the Cold War era, the 'nature' of the new international system and the policies required to promote agents' interests in this 'new' – still vaguely defined – system. Similarly, actors gauged future policy prospects and formulated related vision statements and policies in order to mould the evolving system into one that would be beneficial to them. The immediate post-Cold War era was a generally acknowledged time of transition, while the end point of this process of transition was not in sight. Statesmen were making history, but not under the conditions of their own choosing.

The celebrated end of the Cold War was thus the beginning of a process – both implicit and explicit – of reconceptualising the 'logic' of the international system, the nature of war within it and the determinants of military power. In other words, the end of the Cold War forced a change in the logic according to which states do defence planning and maintain, develop and use their military forces.

The Post-Cold War Era

At the end of the Cold War, Finland quickly "moved to the West". Membership of the European Union and participation in the NATO Partnership for Peace programme were the concrete manifestations of the shift in Finnish security policy outlook from neutrality to military non-alignment. Thus, in the post-

Cold War era Finnish defence policy and the principles guiding defence planning have been defined in close connection – and practically within – the Western security community, while taking distinctive national features into account.

In the 1990s and 2000s, Finnish defence planning and the development of the Finnish Defence Forces (FDF) followed a logic of slow evolution based on the fairly benign security environment of the post-Cold War era. Finland followed the global trend for cashing in the "peace dividend", streamlining the FDF in terms of both its peacetime organization, infrastructure and personnel, and its wartime troop levels and readiness. But the focus of Finnish defence policy remained the prevention of any potential military threats to the nation by maintaining sufficient military capability to repel any attack, even a large-scale conventional military attack. This at a time when most states in Western Europe were transforming their defence planning guidelines in a more revolutionary way, by "going professional" and focusing on out-of-area military operations and expeditionary capabilities.

Gradually, during the first decade of the new millennium, the gap between Finnish defence planning principles and the principles of most of the other Western countries became wide enough to facilitate discussions on the benefits of continuing to rely on general male conscription and maintaining territorial defence against potential large-scale military attack as the framework through which to conceptualize and maintain defence capability.

In retrospect, it might be argued that the US-led Western transformation of the armed forces by exploiting the so-called "Revolution in Military Affairs" (RMA), and the move away from conscription to all-volunteer professional militaries, highlighted the fact that in the defence realm, Finland was getting "out-of-sync" with other Western states. Finland was eager to participate in the development of the European defence sphere, focused mainly on military crisis management, but was doing this on the basis of military capabilities developed solely to fit the requirements of defending its national territory against external state-based military threats. Thus, in the first decade of the new century, Finland faced an emerging "identity crisis". Later events, however, particularly in Georgia in 2008 and Ukraine in 2014, quickly eased most of the concerns that had been growing for a decade and a half.

The geographical and historical relationship with Russia must be taken into account in any analysis of the differences between the Finnish defence planning principles and Western planning more generally, as exemplified by NATO. Directly after the Cold War, Russia was still a great power in a military sense, despite the fact that it had difficulties keeping the peace domestically. In addition, Russia and Finland share a common land border of more than 1000 kilometres. Finns still recall the events of the wars with the Soviet Union in 1939–1945 and the Soviet political and military pressure exerted on Finland during the Cold War. In fact, the threat posed by Russia did not completely disappear in the early 1990s, even though the security situation clearly improved relative to the decades after World War II.

> "The threats to Finland are determined by the country's geopolitical position….The only realistic direction from which a threat could arise is the east, that is from Russia".
> *LtGen (ret.) Ermei Kanninen 1994 (translation by the author)*

> "Although we may not regard Russia as a threat in the political sense, Finland has to develop its defences to allow for all eventualities, including a possible change in the political situation in Russia".
> *Prime minister Paavo Lipponen, 2004 (translation by the author)*

> "Russia is attempting to regain as much as possible of its leading role, resembling the influence that the Soviet Union had in Eurasia".
> *Finnish Security and Defence Policy 2004, Government report to parliament 6/2004*

In the two decades between 1992 and 2012 the peacetime structures of the Finnish Defence Forces underwent several rounds of base closures and the number of paid personnel reduced from approximately 20,000 persons to less than 15,000. At the same time, the wartime strength of the FDF was cut from 540,000 to 350,000 soldiers. The benign international security landscape facilitated the maintenance and development of a defence capability with only a moderate level of ambition. Apart from any potential risks associated with future developments in Russia, there were no significant military threats on the horizon that could be countered using the tools of the FDF. Even military crisis management was becoming a routine mission, and the number of troops deployed and the costs associated with the operations were low compared to the FDF wartime footing and the national defence budget. Procurement decisions were still being based on the logic of national territorial defence.

The surprise

Russia's "warning shot" in Georgia in 2008 was either forgotten or ignored quite soon after by most sections of the Western security community. For Finland, the foundations of its defence planning seemed to have been vindicated post-Georgia. Having sufficient national defence capability to defend its territory and the vital functions of society was still a requirement across the globe, and even possibly in Europe. After all, the war in Georgia took place less than six months after a NATO summit had made a vague commitment to Georgia and Ukraine joining NATO at some point in the future.

Facing economic stresses caused by the global financial crisis in 2008, and facilitated by the seemingly secure international security environment, government decisions were made in 2011–12 to undertake defence reform by 2015. The defence budget was cut by around 10 per cent. As a result, the level of procurement plummeted, the level of daily operations such as conscript training or refresher training was reduced, the number of paid personnel in the FDF was cut to 12,000 and the wartime strength of the FDF was cut from 350,000 to 230,000 soldiers. At the same time, a level of administration – Military Provinces – was cut from the organization of the defence forces and the processes and functions of the FDF were reformed. In sum, the way of doing things and the level of ambition were adjusted to the tight financial situation. The one thing that did not change was the focus of Finnish defence planning: it was still about defending the territory and vital functions of Finnish society against state-based military threats.

The crisis in Ukraine broke out during this reform process. To the surprise of almost everyone in the West, Russia invaded the Crimean peninsula and annexed it. Less than six years after the war in Georgia, Russia had succeeded in modernizing both the equipment of its armed forces and its conduct of operations. In addition, Russia also began a military conflict that was practically a proxy war in eastern Ukraine. Relations between the EU and NATO, and Russia have become extremely strained and dysfunctional. Even communication between the parties – the bedrock of diplomacy – has become cumbersome and almost impossible.

Finnish Defence Policy Today

It is against this backdrop that the 2017 Government Defence Report should be evaluated. The report is the official document that will guide Finnish defence policy for many years into the future, examining the maintenance and development of defence capabilities from the perspective of the next decade. For the first time in the post-Cold War period, the document notes a deterioration in the security environment and increasing military tensions in the vicinity of Finland.

The report notes that given current circumstances, the resources assigned to military defence are inadequate. The defence capability needs to be enhanced at a greater rate than was mandated by the decisions of the 2012 defence reform. In particular, additional funds are assigned to procurement (a cumulative increase of €150 million per year) and readiness (€55 million per year). In addition, the government has stated that two projects linked to future strategic capabilities – replacing the F-18 Hornet fighter fleet and several navy ships, and capabilities connected with the Squadron 2020 project – will be funded by additional resources over and above the base budget. The projected cost of these two projects is €8.2–11.2 billion.

The report does not make any significant conceptual changes to the prevailing defence planning principles. Finland will continue to maintain and develop the defence capability to prevent state-based military threats from emerging and, if necessary, to defeat such threats. In addition, Finland will continue to deepen international defence cooperation and retains the option of applying for NATO membership. The ongoing bilateral cooperation with Sweden is raised to the top of the agenda by the government, as is cooperation with the United States. In addition, the government is removing legislative restrictions on giving or receiving international military assistance.

The change in the international security atmosphere since the annexation of Crimea has resulted in modifications to the Finnish system of national defence. These modifications, however, do not constitute a significant change in the Finnish defence policy outlook or defence planning principles that have evolved throughout the post-Cold War period. The surprise that Russia's actions gave many Western analysts and statesmen early in 2014 – in Finland also - did not result in a need to re-examine Finnish defence policy or the principles on which Finland's defence is maintained and developed. Whether this is due to the strategic competence of Finnish defence policymakers or the effects of inertia in decision-making over the past 25 years is a question best left for future analysis and political debate.

16. The Significance of Defence Research for National Security

Katarina Wilhelmsen and Mikael Wiklund

National security is fundamentally about our Swedish interests; what threatens them and society's ability to meet those threats. Defence and security research plays a vital role in building the capability and readiness needed to ensure our national security, since accessible knowledge defines the limits of both military operational capability and society's general preparedness. Nonetheless, national funding of defence research has decreased by more than 50 per cent in the past ten years. The deterioration in the regional security situation has made the long-term consequences of reductions in defence research more apparent and pressing. The 2016 government inquiry into defence research proposed an increase in research funding. If the results of increased research funding are to have any effect in the near future – that is, within the next defence bill period, 2021–2026 – on the capacity to deal with threats to national security, funding needs to be increased immediately.

National security

The Swedish government's National Security Strategy states that the external threats to society are complex and that predicting exactly which threats will arise is almost impossible. Therefore, to strengthen society, continued knowledge-building, research and technology development must be assured in the long term. In other words, research is central to national security

One way to perceive national security is as the absence of threats against our values, and the ability to ensure that, as a state, we ourselves dictate how society develops. In addition, national security is the absence of fear that our values and way of life will be attacked. National security issues must therefore include strategies for reducing such threats and for being able to return to a condition of normalcy once a threatening development – such as a natural disaster, terrorist attack, military action or some form of economic or diplomatic pressure – has taken place.

The concept of national security can be confusing because it cannot be easily categorised within one single or clearly defined policy area. An issue of national security often originates as an issue of defence, infrastructure or foreign policy and then gains in significance as an issue of national security after it has intersected with other policy spheres. A recent example is how the outsourcing of day-to-day IT operations at Swedish government agencies became an issue of national security. The case illustrated the intersectionality of national security and its relevance at the forefront and as a basis of policy development. Research that supports national security is therefore found in a range of fields. Defence and security research have a prominent role but are by no means alone.

Challenges tied to national security and the role of research

Ultimately, national security is about our values and interests, the threats against them, and society's capacity to meet those threats. This entails specific challenges, where research is an essential part of the solution:

- Society's ability to create national security is defined relative to the perceived threat. If the threats increase while society's capacity is static, capability declines. In other words, it is not enough to maintain capability merely by relying on earlier achievements;

- Society's ability to address threats suffers from a delay. Decisions about developing the appropriate capability must often be made far in advance. Seeking better readiness and increased capability when the need has already become apparent is futile;

- Decisions about future capability requirements are thus by default made in conditions of uncertainty with respect to actual needs. Planning and capacity development in defence and security occur in the face of an unknown and unpredictable future. Structures for working with uncertainty are therefore of crucial importance;

- Society's ability to create national security involves much more than the capabilities of the armed forces. National security is a context in which several different policy areas interact and cannot be managed by the defence authorities alone.

Defence research has a decisive role in satisfying the knowledge needs that arise from the challenges associated with national security. It does this from three different perspectives. The most obvious perspective is to create more and deeper knowledge in areas of known defence capability needs in order to maintain or increase a *capability* over time. This involves advanced, high quality research that moves cutting edge research forward and creates leading experts in diverse disciplines. The results of this research are of vital importance for increasing defence capabilities within the respective areas.

Research, however, is also a tool for creating freedom of action in the face of today's unknown challenges and dealing with uncertainty. Such research is an important complement to research directed at known capability needs, to prepare for unknown threats. This research is not based on clearly defined defence needs, since uncertainty makes it impossible to identify those needs completely accurately. Instead, the research seeks to develop sufficiently good *knowledge* assets in selected areas so that when a capability gap can be identified, that knowledge can be converted into developing capability. Both these research perspectives are important for capability development, and it is important that they can coexist.

Research is also undertaken from a third perspective, where the aim is to create a *deterrent* or *threshold* effect rather than to create knowledge, research findings or problem-solving capability per se. The research, from this perspective, creates a credible picture of a state's potential operational capability. Advanced research of high scientific quality makes it credible that a specific capability might be developed, or that maybe it already exists.

The role of defence research in developing protections against military threats is obvious, but its significance for other dimensions of national security becomes increasingly clear in the boundaries between the civil and the military. This is clear in information and cyber security, for example, where civil society is becoming more and more connected and dependent on the Internet for its everyday functions, while the Internet is also developing as a military arena. Several articles in this issue of *Strategic Outlook* discuss this and related questions.

The particulars of defence research

Defence research has a long tradition. In the 20th century, defence scientists were recruited from academic fields such as chemistry, physics and mathematics. Today, defence research is more specialised and normally focuses on areas not covered by other research providers: war studies, operational analysis, intelligence analysis and research on weapons and electronic warfare, to name a few. This means that defence research acquires a particular importance for national security, since it develops insight in areas where society has no other sources of knowledge.

In the same way that civilian research keeps changing pace with new findings, the defence research area undergoes continuous development. Examples of new fields in defence research include cybersecurity and influence operations as well as the development of unmanned (driverless) aerial vehicles for the military arena. Defence research is “integrity-critical”, since it aims to develop operational capability and is often classified. This secrecy stems not only from the requirements of capability development, but also because the research deals with knowledge that is not suitable for general dissemination, for example for security reasons.

Civil knowledge development is making great advances in some areas that are also critical to defence research. At the same time, however, there are specific defence needs that cannot be met by civilian research institutions. This is partly for integrity and security reasons, but also due to the need for *domain knowledge.* Domain knowledge – knowledge about the environment and activities that will eventually utilize the research results – is in many cases crucial if the research is to generate impact. Specialised research fields, integrity and domain knowledge are reasons why significant aspects of defence research need to be conducted in specialized research environments.

Research: knowledge-based readiness

Research creates an impact when the results – the new knowledge or tools created – are translated into activity. The results do not create a singular, isolated impact but lead to multiple impacts in various places at different times. The impacts of some research are immediately apparent, while in other cases it can take years, or even decades, for the real value to become apparent. There can be no simple predictions about impact or outcomes, and no single measure of impact. Research creates a bank of knowledge – a knowledge readiness – that can be used to resolve various problems at various times. Defence research should thus be considered a readiness, or insurance, to be able to resolve future problems. This implies that a reduced commitment to research entails an increase in future risk.

The use of research results is frequently confused with the research itself; a researcher solving a problem is considered to be conducting research, when he or she is instead applying his or her expertise. The two activities are related but not the same, and one – research – is not the same as the other – problem-solving. Problems can be solved by means of the knowledge readiness that has been accumulated over a long period. Without knowledge readiness, however, current problems would be left unsolved.

If research and problem-solving are confused, this makes it easy to conclude that expertise here and now should have a higher priority than long-term research. This would jeopardise knowledge readiness, and increase future risk-taking as a result. The long-term nature of research also means that it takes a long time for the negative effects of reductions in research on the knowledge base to become apparent.

The erosion of future readiness

Research cycles often have different timelines to policy cycles. Decisions on defence research taken in the context of one defence bill will not achieve their full impact until a later defence bill period. In recent decades, Swedish defence research has experienced major cutbacks, due to assessments of the then current security climate. Many of the effects of these decisions are only becoming obvious now, in a different security context, while others have yet to reach their full impact.

The 2000 defence bill represented a transition from a larger defence system aimed at opposing invasion, to a downsized structure adapted primarily to international operations. The government assessed that the basically positive security situation in Sweden's neighbourhood would prevail, even if some uncertainty remained regarding Russia's political development. The fundamental improvements in the security situation implied that defence expenditure could be reduced without diminishing defence capability. This direction was reinforced in the next defence bill, when it was decided to reduce military defence expenditure even further, including cutbacks on research. Decisions were taken to implement substantial cost cutting in defence research and technical development.

The 2009 defence bill, which was passed after the war in Georgia, identified increased pressures on operational capability and that resources would need to be freed up for this purpose. This meant even further reductions in the funding of research and development. The budgets for 2012 and 2013 also proposed cutbacks on research and development funding.

In total, these reductions have meant that research and development on defence has been cut by more than 50 per cent since 2005, and that long-term research, which is the foundation for the development of future operational capability, has been drastically cut in favour of operational capability here and now. That it has been possible, despite these substantial reductions, to provide any knowledge in support of the development of operational capability is due to the long-term character of research. The knowledge that is the basis for today's capability development contains significant elements of research undertaken in earlier defence bill periods.

The current situation

The world has seen enormous changes since 2000. Threats have developed and today there are advanced military capabilities, as well as the capacity for cyber and influence operations, in our neighbourhood. Current Swedish defence policy designates, as a highest priority, increasing the operational capability of combat units and increasing the aggregate capability of total defence. To ensure the ability of the armed forces to defend Sweden against attack, financial allocations to defence have increased. Before August 2017, however, none of these increases applied to research allocations.

Nonetheless, increasing the operational capability of Sweden's national defence and Sweden's ability to address other threats to national security implies a need to increase research commitments. The 2016 Swedish Defence Research Inquiry concluded that, in the light of developments in the global situation, an increase in resources for Swedish defence research was needed. The Inquiry recommended that allocations to defence research of at least SEK 400 million (around €40 million) should be added to the 2021–2026 defence bill in order to strengthen the capabilities of the armed forces and the aggregate capacity of total defence. The Inquiry also noted that if global developments deteriorated still further, the funding allocations might need to be shifted to an earlier date.

How to reduce Sweden's risk-taking

Global developments have hardly improved of late. If defence research is to have a full impact on capability development during the period covered by the next defence bill, the increase in financial allocations needs to be implemented as soon as possible. A new political agreement to increase defence research allocations from 2018 was reached in August 2017. This agreement cancels the most recently announced cutbacks in defence research and opens-up for recovering also earlier cutbacks.

Increased commitments to defence research entail the creation of sustainable research environments that are allowed the time they need to develop new knowledge in areas specific to defence. Increased knowledge production and research results do not happen overnight, just as increasing the number of teachers, doctors or lawyers cannot be achieved without first increasing the number of students admitted to universities.

Research is all about developing new knowledge or breaking new ground in a certain field. Unfortunately, there are no shortcuts. Well-designed collaborations can contribute to a faster process of knowledge development and provide valuable access to a greater pool of knowledge, but creating viable research environments takes time. Once results have been produced, they must be translated into military capability development, which – like research – is a sophisticated endeavour that cannot be rushed.

Therefore, an increase in defence research must proceed sustainably, with the point of departure being to allow research development the space it needs for the effects of the commitment to become fully apparent. A year or two without any visible impact does not mean that effects will never emerge, but is instead a consequence of the inherent nature of research. To halt the depletion of knowledge – and the long-term security risk-taking that is the effect of reducing knowledge readiness – the increases in defence research and development allocations that have been announced must be carried on for the long-term and from a sustainable perspective.

Authors

Simon Ahlberg has an M.Sc. in Computer Science and Engineering. He is a Senior Scientist in the Department of Sensor Informatics at FOI. His fields of work include geoinformatics and business development regarding the use of geospatial information in the armed forces. His research also includes military modelling and simulation, specifically the rapid generation of 3D environment models through automatic processing of data from airborne sensor platforms. He is also a National Referee with the Swedish Golf Federation.

Maria Andersson is a Senior Scientist in the Department of Sensor Informatics at FOI. She has a PhD in energy systems from Linköping University. Her areas of expertise are methods for extracting critical information from large datasets, and energy-system analysis. She works on national and international projects focused on different surveillance applications, where sensor data are collected and analysed. Maria was previously a VINNMER-Fellow, during which she was a guest researcher at Linköping University.

Erik Berglund is Research Director of the Department of Systems Technology. His main interests are missile systems, air defence systems and weapon system assessment. He is currently on leave of absence working at the Ministry of Defence. Previously, he worked at the Organisation for the Prohibition of Chemical Weapons (OPCW) and Frontex.

Niklas Brännström is acting Head of the Department of CBRN Threats, Dispersion and Radioactive Agents. His field of expertise is atmospheric dispersion modelling. Niklas obtained his PhD in mathematics from the University of Warwick, UK.

Robert Dalsjö is Deputy Director of Studies in FOI's Department of Strategy and Policy and a generalist in politico-military affairs. Robert's current focus is research on Swedish attitudes to NATO, Swedish national interests, Baltic security and Anti-Access/Area Denial (A2/AD). He has previously worked as a Senior Adviser to the Swedish Ministry of Defence and to Sweden's delegation to NATO.

Daniel Eidenskog is a Scientist in FOI's Department of Information Security and IT Architecture. His main work at FOI is research and expert support on information security and IT security for the Swedish Armed Forces and the civil authorities. Daniel has a Ph.D. in computer engineering and a background in the development of IT security products for the armed forces. Daniel's research is partly carried out in the Centre of Excellence for the SCADA project, NCS3.

Martin Hagström is a Deputy Research Director in FOI's Department of Systems Technology. His area of expertise is autonomous systems, aeronautics and unmanned vehicles. His most recent research involves work on autonomous weapon systems. Martin leads the Weapons and Protection programme at FOI and is responsible for the support provided to the Swedish Armed Forces' weapons and protection research planning. He has served in several different positions at FOI and participated in many international research projects.

Eva Hagström Frisell is a Deputy Research Director in FOI's Department of Security Policy and Strategic Studies. Her area of expertise is European security and international operations. She has recently published reports on Germany's and Poland's security and defence policies. Eva has previously worked at the Swedish Ministry of Defence and the Swedish Civil Contingencies Agency.

Alf Christian Hennum has worked as a researcher at the Norwegian Defence Research Establishment (FFI) since 2003. He has a Master of Science in Theoretical chemistry from the University of Oslo. At FFI, he has worked as an operational analyst, mainly on long term planning at the strategic level. He has also studied land warfare, air defence, helicopter operations, long-range precision weapons and personnel analysis at the operational level. During the development of the most recent Defence White Paper, he coordinated FFI's support to the Ministry of Defence. He currently heads Concept Development and Military Operations, a research programme supporting the Defence Staff and the Joint Operational Headquarters.

Michael Jonsson is a Senior Scientist in FOI's Department of Strategy and Policy. His area of expertise is interstate conflicts and non-military security threats. He has recently published studies on Somalia, Nigeria and Syria, and contributed to a report on security and defence policy in northern Europe. Michael holds a PhD in political science and has worked as a consultant for the International Monetary Fund and an operations analyst at the Swedish Defence Headquarters. He edited Conflict, Crime and the State in Postcommunist Eurasia (University of Pennsylvania Press, 2014).

Farzad Kamrani is a Scientist at FOI in the Department of Decision Support Systems. He has worked for many years on modelling and simulation, and his research interest is in the field of artificial intelligence and machine learning. He is also interested in data security and privacy. He has a Master's degree in Computer Science from the University of Gothenburg and a PhD in Electronics and Computer Systems from KTH.

Anders Lennartsson is a Deputy Research Director in FOI's Department of Systems Technology. His area of expertise is aerospace technology, including missile weapons such as ballistic and cruise missiles, and missile defence. On behalf of the Swedish Ministry for Foreign Affairs, he Chairs the technical experts' working group of the Missile Technology Control Regime (MTCR).

Fredrik Lindgren is currently on leave of absence from his position as a Deputy Research Director in FOI's Department of Societal Security and Safety, working at the County Administrative Board in Uppsala. His focal areas are emergency preparedness, civil defence and total defence. He has in recent years acted as project manager on several projects on civil defence and has also worked on studies of the Swedish system of emergency preparedness at the national level. He previously worked at the Ministry of Defence.

Sandra Lindström is a Senior Scientist in the Department of Naval Systems, where she is currently the Deputy Head of Department. Sandra has worked at FOI for 15 years, during which she has coordinated and managed the space research group and different space projects for customers such as the Swedish Armed Forces, the Swedish Defence Materiel Administration and the Ministry for Foreign Affairs. Sandra holds an MSc in Space Engineering from Luleå University of Technology.

Peter Nordlund is Research Director in FOI's Department of Defence Economics. He leads different defence economics projects covering a broad range of topics. He worked for almost two decades in managerial positions in the banking and finance sector.

Tore Nyhamar has worked in the Norwegian Defence Research Establishment (FFI) since 2001 as a project leader and researcher. He obtained his doctorate from the Department for Political Science at the University of Oslo where he held various positions from 1989 to 2001. In his work at FFI, he has led the research on international operations, editing two books on the topic, most recently International Military Operations in the 21st Century: Global trends and the future of intervention. His current research is mainly focused on military operations by small states and the protection of civilians in military operations.

Torbjörn Nylén is a Senior Scientist in FOI's Department of CBRN Threats, Dispersion and Radioactive Agents. His area of expertise is internal dosimetry and radioecology. He is also the scientific lead on radioactive substances.

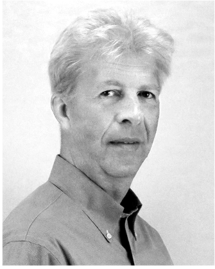
Jyri Raitasalo, LtCol, PhD, is Senior Staff Officer in the Planning Unit (strategic planning) of the Finnish Ministry of Defence. He holds the title of Docent of Strategy and Security Policy at the Finnish National Defence University. In his most recent assignments he has served as the Commanding Officer of the Helsinki Air Defence Regiment (Armoured Brigade), Head Lecturer on Strategy at the Finnish National Defence University, ADC to the Chief of Defence and Staff Officer (strategic planning) in the Finnish Defence Command (J5). Jyri Raitasalo is a member of the Royal Swedish Academy of War Sciences.

Henrik Ramebäck is a Research Director in FOI's Department of CBRN Threats, Dispersion and Radioactive Agents. His area of expertise is the identification, measurement and characterisation of nuclear and radioactive materials. Henrik is also an adjunct professor in nuclear chemistry at Chalmers University of Technology.

Niklas H. Rossbach is a Senior Researcher in the Department of Security Policy and Strategic Studies, focusing on US and European security. He has written about "Brexit" and the strategic consequences of the new US energy production policy. He holds a PhD in history from the European University Institute and, with the support of the Axel and Margaret Ax:son Johnson Foundation, he has been a Visiting Fellow at the University of Oxford Changing Character of War Programme, researching psychological warfare.

John Rydqvist works in FOI's Department of Security Policy and Strategic Studies. He currently heads the Defence Policy studies project at FOI. He headed the Asia Security studies project in 2006–2015. John has published research on the strategic balance in the Asia-Pacific/South Asia/Middle East crescent. His special focus is strategic weapons modernisation and force transformation. He is currently researching nuclear weapons in the trans-Atlantic theatre.

Anna Sundberg is a Senior Analyst in the Department of Security Policy and Strategic Studies where her focus is on the security and defence policies of European states. She has recently published reports on Germany's and Poland's security and defence policies. She has also written a number of reports on the EU. Anna has worked at the Swedish National Defence College, the Ministry of Defence and the French research institute Fondation pour la recherche stratégique.



Ulf Söderman is a Deputy Research Director in FOI's Department of Sensor Informatics. Ulf's main interest is geoinformatics with a focus on new types of geographic information in 3D and their application to the Swedish defence. He has previously worked on 3D-mapping and the production of digital 3D-landscapes models. He has a M.Sc. in computer science and engineering and a PhD in computer science from Linköping Institute and of Technology.

Gustav Tolt is a Senior Scientist and Project Manager in the Department of Sensor Informatics. Gustav works mainly on the development of analysis methods for 3D geographical information and data from 3D imaging laser sensors. He has a Masters Thesis diploma in Engineering Physics from Chalmers Technical University, Gothenburg, and a PhD in Industrial Measurement Technology from Örebro University.

Mikael Wedlin is a Deputy Research Director in FOI's Department of Information Security and IT Architecture. His main focus is IT weapons and IT warfare. He has also carried out research on security in critical infrastructure systems and had a large part in the development of the FOI Cyber Range, CRATE.

Lars Westerdahl is a Scientist in FOI's Department of Information Security and IT Architecture. His area of expertise is information security. For the past three years he has been coordinating the department's work with the National Centre for Security in Control Systems for Critical Infrastructure (NCS3), which is part of the Swedish Civil Contingencies Agency's programme to increase security in industrial information and control systems. Lars has previously worked on access control issues, as well as information security issues for IT systems during development and operation.

Erik Westring is a Research Engineer in the Department of Information Security and IT Architecture. His area of expertise is information security for critical infrastructure. He is active in and publishes reports for NCS3 in conjunction with the Swedish Civil Contingencies Agency (MSB). He has jointly developed and run larger national/international Information security exercises.

Katarina Wilhelmsen is the Director of Research & Development at FOI, with responsibilities for research planning and evaluation. She has also worked on similar issues within the Swedish Armed Forces. In 2016 she acted as secretary to the government committee on defence-related research and development in Sweden. Her current research interest concerns multilateral verification of nuclear disarmament. Katarina holds a PhD in physics from Chalmers University of Technology, is an associate professor in physics at Stockholm University and has been an adjunct professor at Chalmers.

Mikael Wiklund is an Analyst in FOI's Department of Strategy and Policy. His area of expertise is strategic management of governmental agencies with a particular interest in defence policy, and the economics of defence and intelligence. He has recently been active in strategy development and risk management for the Swedish Armed Forces. Mikael currently serves at the Swedish Armed Forces Headquarters as an Operational Analyst.

Mike Winnerstig, PhD, is a Deputy Director of Research in FOI's Department of Security Policy and Strategic Studies. His research has long focused on the foreign, security and defence policies of the USA, and on NATO and related transatlantic security issues. Since 2010 he has also studied the security issues of the Baltic Sea area, especially the defence and security policies of the Baltic States. As a FOI employee, he has also served as an embedded analyst at the Swedish Ministry of Defence

Ann Ödlund is a Senior Scientist at FOI's Department of Strategy and Policy. Her educational background is in behavioural science and organizational psychology. In recent years she has worked in the areas of total defence and civil defence, and has published several reports on these subjects.

Editors

Daniel Faria is a Senior Analyst in FOI's Department of Naval Systems and co-editor of Strategic Outlook 7. He is responsible for research projects in the fields of space security and military space capabilities, while also acting as a technical adviser to the Swedish Ministry for Foreign Affairs. Daniel holds an MSc in physics and a PhD in astrophysics from Lund University. Before taking up his current position at FOI, he had a career in operational analysis and research policy.

Cecilia Hull Wiklund is the Project Manager and Chief Editor of Strategic Outlook 7. She is a Senior Analyst in the Department of Security Policy and Strategic Studies and Team Leader for FOI's Studies in African Security. Cecilia has previously been seconded to the Ministry of Defence, working on international operations and Africa. She has also worked on identifying lessons learned within the Swedish Armed Forces and on peacekeeping evaluations at the United Nations.

Bengt Johansson is a Scientist in FOI's Department of Societal Security and Safety and associate professor in Environmental and Energy Systems Studies at Lund University and co-editor of Strategic Outlook 7. His area of expertise is energy and climate policy and in recent years he has directed his interest to how energy security is being affected by the current transformation of the energy system.

Josefin Öhrn-Lundin is a co-editor of Strategic Outlook 7. She is a Junior Analyst at FOI's Department of Defence Economics. She holds an MSc in Economics of Innovation and Growth from the Royal Institute of Technology.

FOI

ISSN1650-1942

www.foi.se