Strategic Outlook 9

Future Threats

Jenny Lundén, Anders Melander, Elin Hellquist, Björn Ottosson, Anders Strindberg and Liselotte Steen (ed.)

FOI-R--5190--SE

JULY 2021

Strategic Outlook 9

Future Threats

Jenny Lundén, Anders Melander, Elin Hellquist,
Björn Ottosson, Anders Strindberg and
Liselotte Steen (ed.)

July 2021

FOI-R--5190--SE

ISSN 1560-1942
Printed in Stockholm 2021 by Swedish Defence Research Agency, FOI
Cover: Shutterstock
FOI-R--5190--SE
Approved by Malek Finn Khan

Strategic Outlook 9 Future Threats

Foreword

Where are we heading? This question is repeated again and again in millions of Swedish homes every year in the popular TV game show, *"På spåret"*, in which contestants are trying to figure out the destination of a train journey as quickly as possible. When we try to understand which threats we will face in the future, there is no omniscient judge who can set us on the right track and quickly give us the correct answer. Even though we don´t have all the answers nor a judge to help us, we have nevertheless tried to answer the question of where we are going. Will we face supersoldiers in the future? What military threats are emerging and will future social media algorithms be used to influence our reality at a scale that is far greater than today? Is it possible today to discern what will threaten us in the future by looking back and by contemplating our present world? In addition, the article by researchers at the RAND Corporation, in the United States, adds further perspectives on how threats develop over time.

Another author uses the term threat cascade, which captures very well what we have to deal with. Even if actors and threats change over time, the total defence system must function across and between different sectors of society. To be able to confront, push back and defeat a competent enemy is a decisive piece of the puzzle. Unfortunately, antagonistic threats are always going to target the areas where we are the weakest. Through research, development, analysis and cooperation, we can contribute to a more robust society. Your task as reader, when you join us in our leap into the future, is to ask what other threats must be taken care of.

Stockholm 2021

Jens Mattsson
Director-General

Content

Introduction

Preparing to confront and deal with threats is no easy task. On top of that, when they are lying in wait in the future, we also have to identify which threats are possible, and which are probable or only fantasies. Despite that, or perhaps because of it, it seems that many of the threats described in science fiction have found their way into reality, albeit in smaller and more modest forms.

But what might the threats of the future look like? The media and popular science bring it up frequently, but often limit their attention to what is in vogue today, for example hybrid and cyber threats. In Strategic Outlook 9, we wish to broaden the horizons and bring up what is perhaps being overlooked. In their articles, FOI's researchers have looked ahead and described conceivable future threats. The picture that their contributions paint is broad, since there is no clear-cut definition of either the threats or the future.

In the first article, one can read about how the view of future threats has changed through the years. *Perspectives on future military threats* presents the structured work that has long been carried out within the Swedish Armed Forces with the support of FOI. Through the study, the perspective is focused on future threats in order to create concepts and build capabilities that aim to support the development of our defence as it faces the future. But will future wars be conducted in outer space, or are we already moving towards that? Our modern society is already dependent on satellites, which makes us vulnerable to conflicts in space. These developments are highlighted in the article *Space is a warfighting domain*.

Seen from a global perspective, when the world order that we have become accustomed to undergoes changes, we can also experience the changes as threats. These can involve changes in international relations, weakened alliances, or new cooperation on security policy. These perspectives are examined in *Threats against the West and the future of transatlantic relations* and in this edition's guest contribution, which is from RAND Corporation. In their article, *Future Threats and Some Considerations for the Next U.S. National Defense Strategy,* RAND's researchers take the American national security strategy as the point of departure for their discussion of how a future version of it can be configured to contribute to global security.

Even democracy itself is threatened, a concern discussed in the article, *Democratic security: Confronting silent threats against society's fundamental principles.* This is an elusive and almost intangible threat that is comprised of many different components. The article's approach is broadened beyond the normal boundaries that are usually found in this research field. Another article grapples with whether or not our language is sufficient for communicating when threats fall outside the scope of our own understanding – somewhere in the grey area between cyber and the physical world. In other words, are we capable of comprehending threats on a conceptual level? These challenges are discussed in *The threats of the future – Do we see them coming?*

Another matter is that decisions are almost always associated with uncertainty. This applies especially when decisions are being taken to confront future threats that are in themselves highly uncertain. This difficult task is taken up in the article, *Robust decisions for managing a changed climate.*

Just as climate has a global dimension, so too does the threat to health, which is influenced by both international politics and disinformation. Additionally, there is a worrisome tendency towards a growing willingness to use biological and chemical weapons. This topic is the subject of two of the articles, *A threat cascade against global health in the era of disinformation,* and *Future antagonistic biological and chemical threats*. In these fields, the advancement in technology is both a blessing and a curse, as it can increase the threat, but at the same time create tools to counteract the threat.

Technological development promises to deliver opportunities that will be useful for us in the future. Artificial intelligence (AI) certainly has great potential to simplify everyday life, but what risks does the technology bring? Some of the threats are addressed in *AI and influence operations in social media.* Other technologies, which are easily accessible to anybody, for example the popular hobby drones, can be modified for use in conflict and war. One can read about it in *Swarming drones – a realistic future threat?* Science fiction has perhaps made it easier to imagine how lasers can be used as weapons. How such a weapon might work is discussed in the article, *Can laser weapons be a game changer in future conflicts?* Even more like science fiction is so-called human performance enhancement where soldiers are equipped with exoskeletons and implants, or have their performance enhanced with the aid of chemicals; this is technology that is catching up to fiction. Some of these futuristic visions are presented in the article *Supersoldiers.*

For those who might wish to learn more about any of the topics raised in Strategic Outlook 9, each article closes with several tips for further reading.

The editors

1. Perspectives on future military threats

Riitta Räty, Göran Kindvall and Ann Ödlund

It is genuinely difficult to study the future, especially when it regards a threat posed by a determined and well-resourced antagonist. When it comes to assessing possible future threats and which of them could actually be realised, one needs to navigate between the expected and the unexpected. There is a need to identify which threats are trending now and which are being downplayed, and the reasons for these choices. It is also important to try to understand which threats are just fads, only to more or less disappear; which threats are just emerging and which are about the same as before. This article is a reflection over the assessment of future military threats and how the Swedish Armed Forces has viewed these from the Cold War forward.

The Defence outlook – Looking ahead 20 years to give advice today

Understanding which future threats Sweden may be encountering and how they should be handled are important questions in developing the country's total defence. Assessments of what can be expected in the future help today's decision-makers to make important choices about the coming needs. Decisions often involve major long term investments, and therefore it is important to consider possible future developments and make better choices. In its long-term defence outlook, the Swedish Armed Forces has been examining this in a military perspective for decades, to provide knowledge and context to the long-term decisions that need to be taken in the near future.

The Swedish defence outlook is conducted in multiyear cycles for the purpose of, among other things, supplying information in support of the defence bill that is adopted by the parliament every five years. This is done in parallel with implementing the current defence bill. The long-term study can be seen as consisting of four parts: futures-oriented strategic intelligence analysis, creation of defence concepts with a scope of about 25 years, development of alternative armed forces structures within a 15-year frame and, finally, advice to the approaching defence bill.

The strategic intelligence analysis in the current defence outlook, that is, in preparation for the 2025 defence bill, takes a broad perspective on developments towards 2045 and what can affect Sweden's security. This comprises analyses of global trends, security policy, opponents, partners, societal change, military technology and future operation environment. The strategic intelligence analysis identifies future drivers, challenges and threats and is used to create a set of scenarios that attempt to capture uncertainties about the future. The scenarios are used to visualise and illustrate military problems and contribute to formulating ideas for future solutions to them, so-called defence concepts. The next step further elaborate these ideas as armed force structures, paying attention to both the legacy from current armed forces, capabilities and long-term commitments within personnel, materiel and provision of infrastructure. These alternative structures envision the way the Armed Forces might look in various future configurations. The capability of the structures to deal with different threats is then evaluated, for example through war gaming. Finally, there is an analysis of how future defence capability can be achieved and which decisions are needed now in order to realise it.

In the last defence outlook, 2016–2018, in preparation for the 2020 defence bill, Russia's geopolitical interests and military activities continued to represent the dominant challenge in the Baltic Sea area. It points out, however, that some uncertainty prevails about Sweden's security policy, since the global security environment is changing. It further observes that the pace of technological development means that the Armed Forces should pay acute attention to the threat from the space and the cyber domains, and that hybrid threats in peacetime poses new demands.

It can nevertheless be considered that many of today's threats have long been discussed and are well-known. Looking back at earlier assessments and how the situation has changed can provide perspective and lessons for today's standpoints.

Looking back

During the Cold War, the assessment of the security situation in Europe was characterised by stable relations. Developments were steered by the political and military interests of the superpowers. The defence outlook from 1975 described the threat as clear and stable. There was a classic invasion threat to plan for, but the threat level was varied. The threat of nuclear weapons was a reality that had to be accounted for, as was the threat of a surprise attack. The total defence that existed during and after the Second World War was comprehensive and considered sufficient for meeting a large-scale armed invasion that would amount to an attack against the entire society.

The 1987 defence bill was the beginning of a number of cutbacks in the military defence organisation, prompted by among other things an under-financed defence bill but then accelerated with the fall of the Berlin Wall and the dissolution of the Soviet Union. After a few initial years of turbulence, the new security situation led to the assessment that there was no longer any substantial military threat against Sweden. Invasion-oriented defence was thus seen as out-dated and too large. This in turn led to a dismantling of the total defence system. The 1997 defence outlook, during the transition from invasion defence to the following much smaller defence focused on peacekeeping operations abroad, discusses a broader range of threats and risks. Like today, what is currently called hybrid threats are discussed: "Attack methods that in themselves can range from hidden information operations to different forms of armed operations – sometimes attributable to a national military source – sometimes with more indefinite sources". The broader threat range became clear in the 2006 defence outlook, which spoke of dealing with threats across the entire scale, from crisis management at low conflict levels to all-out war against a high-tech enemy. It spoke of threats against global flows and rapid event escalation, and that events in distant parts of the world can have consequences even nationally.

Future threats from technological development

It is considered that technological development will have major impact on both the emergence of potential threats posed by an adversary and for the development of not only military defence but also the entire total defence. Today's discussions revolve around the influence that artificial intelligence, automation, biotechnology, quantum technology and several other technological areas can have in the future, both on society in general and on military capability. These and other technology areas are monitored for so-called disruptive technologies, that is, technology that in some way involves a revolutionary breakthrough and that could either entirely or partially change the conditions for an armed conflict: an exciting development for some, a nightmare for others. Will those who dominate be the ones who have the most cutting-edge artificial intelligence, or those with quantum technology based systems? What will happen if people to a great extent disappear from the forward battlefield and are replaced by unmanned or autonomous systems? Or if a superior artificial intelligence also actually takes decisions on operations? Or what if quantum computers break today's encryptions, or performance-enhancing technology and equipment make superhuman soldiers possible? Some of these applications are already being discussed today from legal and ethical perspectives.

Disruptive technological breakthroughs are nothing new. History is full of them. Two examples that clearly affected the military's effectiveness are gunpowder and nuclear weapons. Are we headed towards similar breakthroughs now? And what does that mean for how we view future threats?

Studies show that in principle it isn't so difficult to state which technology areas are interesting. What is difficult is knowing exactly which applications might be useable and for what. It is also difficult to know when the technology is available and which problems need to be solved along the way.

Development of the threat from a futures perspective

Armed attack and the opponents military capability have traditionally completely dominated descriptions of the conflict environment that the Armed Forces are to operate in. The attacker has been known and technologically and numerically superior, and the level of violence has been high. Today, the focus is as well on an attack against Sweden by an unknown sender, in the grey zone between war and peace. An enemy can, today, not least because of technological progress, use relatively small means, accurately achieve their aims and thereby avoid an escalation that leads to armed conflict. Attacks can be conducted with different degrees of intensity and consist of for example sabotage, influence operations and cyberattacks directed primarily at civilian targets. One question is how such attacks should be handled. Another question is how total defence's current toolbox needs to be strengthened. What is clear is that coordination and cooperation within the frame of total defence will be increasingly important in identifying an attacker and in confronting an attack that occurs in peacetime, without decisions on heightened alert being taken.

Reflections about future military threats

Assessments of potential military threats have been central for the financing and direction of defence; this has entailed major swings between development and dismantling and led to major gaps in the total defence system. The Swedish Defence Commission's reports show that today there is a political will to commit to a basic capability that needs to be consistently in place over time, whatever the current threat.

In developing future military capability, it is important to take a broad look at potential military threats, especially the palette of resources available to an antagonist. Threats need to be understood from a variety of perspectives. What happens, for example, when an antagonist is technically more advanced and better trained? An emphasis on greater quantity may then be inadequate. On the other hand, a commitment to quality could result in so few resources that it becomes a weakness in its own right.

Much of today's reasoning around threats is familiar from earlier assessments. Threats and risks are deemed as affecting the entire societal structure; it is expected that an opponent will take advantage of society's sensitivity by attacking vital functions. One should not forget that military resources probably will be used against civilian as well as military targets. Thus, awareness of military threats become relevant not only for the Armed Forces but for other actors as well.

In conclusion, in futures studies it is easy to drown in uncertainty both about the future itself and about possible future threats. Some things can be handled by gathering information, whereas other things are genuinely uncertain and make it necessary to search for solutions that can handle unforeseen events. It is reasonable to begin the analysis with whatever is least uncertain, investigate the conditions of various future circumstances and allow that which is more uncertain appear clearly in the final result. This also implies that one needs to prioritise among the threats and begin with those that seem most certain. This emphasises, as well, the importance of working with flexible strategies that can be adapted to meet different global developments. Such analyses are part of the defence outlook's role in the development of military defence.

In a defence outlook, studying future development and threats provides the possibility to evaluate today's solutions in the light of possible future threats. Such studies should also be undertaken within civil defence. Looking at other threats than those that are at the top of today's agenda provides a basis for a more robust total defence that is relevant over time. History shows that it is easy to end up in a blind alley; the kind of futures-oriented work described here allows the possibility of countering that tendency.

FURTHER READING

Kindvall, Göran, Lindberg, Anna, 2020, *Militärteknik 2045 – Ett underlag tillFörsvarsmaktens perspektivstudie,* FOI-R--4985--SE.

Kindvall, Göran, 2019, *Hur kan den framtida operationsmiljön se ut?* FOI Memo 6844.

Försvarsmakten, 2018, *Tillväxt för ett starkare försvar*, FM2015:13192:15.

2. Threats against the West and the future of transatlantic relations

Niklas H. Rossbach

In 2014, only weeks before Russia's aggression against Ukraine, Sweden's then prime minister drew the conclusion that, "Cooperation in the EU and NATO has made it difficult to imagine any decisive military threat against any country in Europe." In hindsight it is of course easy to know better. Linear thinking often works well, when tomorrow is expected to be like today, but not always. To forget centuries of conflict-ridden European history and claim that war in Europe is practically impossible is always reckless.

A major challenge to the West's cohesion in security is whether it is ready to face both new and old security threats. Envisioning threats require imagination. Without it, it is neither possible to understand global developments, nor to prepare for the danger of revanchist great powers. A lack of imagination easily result in failed preparedness, something that could affect the whole process of restarting Sweden's total defence concept, a civil and military whole-of-society approach. In order to raise awareness of different future risks one starting point is to imagine three distinct scenarios regarding the West's most important relationship, namely the one within the West itself, between the USA and Europe: the transatlantic relationship.

Cohesion is beginning to crack

The financial crisis that broke out in 2008 sowed doubt about the West's cohesion. For revanchist great powers, such as Russia, the crisis wakened hopes of being able to challenge the Western-led international rules-based order. The West's core has long been comprised of the USA and Europe. During the Cold War – after two bloody world wars and thanks to a non-European great power, the USA – the democracies in Western Europe began to promote European integration. At the end of the Cold War, continued European integration was a central part of the Western led international rules-based order, wherein global trade was promoted, world peace was secured and smaller states won influence, thanks to multilateral cooperation.

After the 2008–2011 economic crisis, successive geopolitical challenges have followed. Russia unexpectedly annexed Crimea in 2014. The United Kingdom voted in 2016 to leave the European Union. It is likely that the economic crisis contributed to the country's growing scepticism towards EU. Whatever the causes, Brexit is a significant geopolitical setback for the EU, since a consequence is that the union loses one of two great powers that have the capability to deploy military forces to distant destinations overseas. The election, in 2016, of Donald Trump as USA's president also astonished the world. That he in addition, like his predecessor, often focussed on Asia, also surprised many observers.

The constant dilemma for Europe's defence policy development has been that if the NATO allies in Europe do less than what the USA wishes to them to do, in the form of defence commitments or combat operations, then this worsens transatlantic relations. But if Europe instead increases its own military capability within the EU, this can also irritate the USA, who is protective of its leading role in the West.

Dealing with revanchist great powers

Neither the annexation of Crimea nor Russia's continued aggression against Ukraine has succeeded in splitting the West. The Swedish Defence Commission has pointed to the risk that more conflicts between the West and revanchist great powers can occur simultaneously in the future. This could be the result of Chinese aggression in the Far East and the USA being forced to focus on China. This could provide Russia with the opportunity to take its military adventurism one step further in Europe. Such a situation, or a similar one, makes it necessary for Europe to be able to defend itself to a much greater extent than previously expected. Despite the presence of American forces in Europe, US armed forces may need to concentrate on helping the American allies in the Far East. Thus, Europe's defence needs to be strengthened, but in the present situation that is in itself a security policy challenge for transatlantic relations.

If Europe in the future needs to maintain its own security to a greater extent than it does today, there are three alternatives: restore traditional transatlantic relations, promote itself as a more equal partner of the USA, or take its security into its own hands. The first option seems to be what is currently going on. NATO is re-arming and focusing on traditional territorial defence, i.e. the defence of the European members of the alliance. These developments are dependent, however, on the ability of the American forces to deal with more than one large-scale military conflict against a peer military power at any one time and, additionally, on Europe and the US having the same geopolitical priorities, which might no longer be the case.

The second alternative would be to deepen transatlantic relations by for example reviving the free trade agreement, the Transatlantic Trade and Investment Partnership (TTIP), between the EU and the USA. This would make the EU a more equal partner to the USA. A new TTIP initiative would increase the USA's interest in Europe's economy and accordingly European security. Another possibility would be to create a so-called European pillar within NATO, in which the European NATO members had their own distinct role. But a stronger European NATO does not strengthen the EU's position. Regardless of whether the second alternative strengthens the EU or NATO, Europe as a whole would still need to ensure its own defence capability when faced with a great power conflict, at least to gain time until help arrived.

The third alternative primarily involves the EU's taking on greater responsibilities. This is often associated with vague visions characterised by such slogans as, for example, "strategic autonomy". The risk with such visions is that Europe is repelling its closest partner in global security, the USA, at the same time as it, for economic reasons, increases its dependence on Russia and China, whose energy exports and trade, respectively, Europe needs. Such visions can weaken Europe's defence before a viable European military capability is in place. This is a dilemma for visions that are supposed to justify European defence cooperation and reinforce Europe's security.

Network-based security policy – A fourth alternative?

The geopolitical surprises have contributed to a number of different defence and security policy initiatives. Together, these can be considered as a fourth alternative, even if that is not the intention with the individual initiatives.

A few examples of initiatives include the EU's development of defence capabilities, such as the Permanent Structured Cooperation (PESCO). The United Kingdom has used its own contingency force, the Joint Expeditionary Force (JEF), as its own forum for cooperation and in order to create close ties with countries that are willing to contribute to the force's resource pool. France has launched another initiative, the European Intervention Initiative (EI2), which among other things is supposed to contribute to a common European strategic culture, for example through coordination around threat scenarios. Sweden is participating in all of these multilateral efforts and in addition the country is one of NATO's partners. At the same time, the EU and NATO are increasingly cooperating on so-called hybrid threats, such as disinformation.

During the Cold War, overlapping international organisations and multilateral fora created a European security architecture that contributed to security not only in the West but also, eventually, in all of Europe, at least, that is, until the annexation of Crimea. In the past the architecture's stability stood in contrast to other parts of the world that lacked an equivalent number of overlapping security related institutions.

The potential threats from revanchist great powers are shared to a greater or lesser extent by all countries in the West. If it were possible to link all the new initiatives, it could result in a modernised security policy architecture that could be likened to a network-based security policy. Cooperation between the various initiatives will perhaps become easier when they have more fully matured. An established Western network-based security policy assumes, however, that all, or in any case many, western-European countries participate in most of the cooperation efforts and that the new initiatives become mutually reinforcing, instead of competing with each other. With this kind of comprehensive cooperation, the security of countries in the West could increase, since the participating countries would always have the opportunity to utilise some part of this new security policy net.

This kind of network thinking assumes, perhaps, new flexible ways to rapidly coordinate the West's foreign and defence policy. New security policy routines and forms of cooperation have been created before, when a common threat made it necessary. This happened, for example, when NATO was formed to protect Europe from the Soviet Union. For those countries who are members of both NATO and the EU, there is also experience to build on. In practice, a joint development and cooperation between all initiatives could involve a renewal and updating, respectively, of the old European security architecture and transatlantic relations.

If cohesion cracks

If Europe does not succeed in strengthening its own defence capability, the West's leading role in the world risks being a thing of the past. Without both a strong USA and Europe that can support each other, it will be more difficult to uphold mutual interests, such as the international rules-based order. If the future instead involves a multipolar world of equally strong great powers, the USA can probably succeed in being the leader among equals. On the other hand, a more independent EU is at risk of having a harder time asserting itself when being an economic great power is no longer sufficient to gain influence in the world.

Neither the EU, NATO, nor Sweden can move forward merely by dusting off and upgrading plans from the Cold War. The next war is never like the previous one – this is also true for cold wars and grey-zone conflicts. It is useful to remember Clausewitz's aphorism, "War is the continuation of politics by other means". Revanchist opponents are using their imagination, for example by using disinformation and attempting to redraw Europe's borders. So far, both EU and NATO are still with us, but they have not shown that they are preventing the West's enemies from using their imagination.

In addition, the world is on the threshold of a new digital technological era, for example thanks to cyber and artificial intelligence, but especially since already ongoing technology trends are changing our culture including the nature of warfare. Russia and China are already trying to achieve their political objectives by other means than purely traditional uses of military power. For example, they use influence operations, such as manipulations of democratic elections in other countries. Such efforts are more cost-effective and less risky than a nuclear weapons arms race or a *blitzkrieg*. Our readiness must continue, however, to heed the threat that often seem the most improbable, a new major war.

More than a hundred years ago, the most initiated observers believed that technological developments had rendered war impossible: there would be too many casualties and the war risked being static and altogether too economically expensive. Despite the fact that these respective predictions proved accurate, the First World War demonstrated that war could break out, anyway, and continue for years. As noted in traditional *realpolitik,* it is not always the most noble nor best ideas that win approval in international politics. Instead, bad ideas often attract many adherents and the decisions that follow can have the most unpredictable consequences.

The way forward

Today, the greatest risk presented by countries such as Russia and China is that they can attempt to pursue bad ideas about aggressive expansion and assertions of spheres of interest, and so on, with the aid of new technology. They are developing new capabilities that can be used, with or without open military warfare, to undermine the West's freedom of action in security policy. Accordingly, the West must ensure that it retains a lead in the development of technology.

Technological development can contribute capabilities that can deter new types of attacks or ward off attacks in new arenas, such as the cyber arena. In addition, technological cooperation between Western countries could strengthen new security policy initiatives and, eventually, the emergence of a new security network based on the West, or democracies more broadly. Technological cooperation can counteract the fragmentation of the West and the cooperation between democracies. But the objective should not be a technology arms race that only leads to a political impasse between the West and its enemies.

In its striving for greater security, the West needs to avoid militarising society to the degree that it risks undermining the very values the West wishes to preserve. For the West, technological development can be a means for promoting trade and continuing global peace based on the international rules-based order. A modern and effective Swedish whole-of-society, i.e. total defence, effort, has to make certain that relevant technological developments are consistent with a realistic security policy analysis of global trends that pays attention to the enemy's intentions and behaviour. In other words, a cohesive West, including a functioning Swedish total defence, requires imagination on the part of both engineers and analysts.

Further reading

Rossbach, Niklas H., 2019, *USA:s framtida säkerhetspolitik – på 30 års sikt.* FOI Memo 6784.

Rossbach, Niklas H., 2019, *Whither transatlantic security? Values, interests and the future of US-European relations,* FOI-R--4869--SE.

Rossbach, Niklas H., 2018, *The geopolitics of Russian energy – Gas, oil and theenergy security of tomorrow,* FOI-R--4623--SE.

3. Democratic security
Confronting threats against society's fundamental principles

Anders Strindberg and Erik Svensson

On a fundamental level, the democratic freedoms and rights of citizens and the ability of government authorities to secure the population's security and wellbeing are national interests in their own right; that is, they are the core of what is to be shielded from assault. These protection values, however, have common vulnerabilities that are continually under attack. The concept of "democratic security" describes a primarily social science-based research approach within FOI that views democracy and threats to democracy as connected elements within a system. The purpose of this approach is to better understand the connections between different vulnerabilities and the relations between various threats, in addition to stimulating new critical thought on countermeasures and their consequences. The question of how the state and society can confront threats against fundamental values without harming them in the process is a pressing challenge that requires a broadened perspective.

Vulnerabilities and threats

Our democratic freedoms and rights, the ability of government authorities to conduct their missions and the state's trust capital are intimately interconnected; as values to be protected but also through their vulnerabilities. It is clear that they are increasingly the targets of so-called asymmetrical threats. This can involve foreign powers who in times of peace or crisis use different forms of information warfare to divide Swedish society and weaken the state, in order to improve conditions for their own strategic objectives. This can also involve domestic actors, who through coercion or violence try to force societal changes in line with their own special interests. Information warfare, violent extremism, hate crime, serious organised crime and honour-related violence and oppression are examples of the spectrum of activities that constitute a concrete threat, not just against individuals, but also against the fundamental functions and principles of civil society.

Researchers have pointed to increasing social and political polarisation in the West, including Sweden. For the individual, the experience of not understanding complex societal challenges, such as migration or increasing criminality, can create emotional reactions such as frustration, dissatisfaction and anger. So, too, the feeling that oneself or one's group is marginalised or disadvantaged through for example unemployment or social alienation. Such reactions can lead the individual to search for simple explanations and solutions. The opportunity to channel these emotions – against other social groups, the state and authorities, or society's fundamental principles – is an elementary tool for both foreign powers conducting influence operations and violent extremists in the process of building their networks.

Disinformation

The media and propaganda resources of other states are part of the Swedish information environment and social debate. When they are used clandestinely and with antagonistic intentions, however, one may speak of influence operations. Through fake news and other disinformation efforts, such activities often take aim at the most inflamed parts of social discourse. Disinformation is tailor-made in so-called troll factories by the intelligence services of foreign powers, for the purpose of manipulating ideas and attitudes, contributing to increased social and political polarisation and decreased trust in government authorities and the state. When the tenor of the public conversation becomes so wound up that common ground is undermined and social groups turn on each other, the fabric of society is torn.

Disinformation is spread via fake news sites, social media, or the attacker's own news channels. It is often difficult to determine what is true, distorted, or entirely fabricated. It is even more difficult to discern who is behind a claim, a tweet, or an article. In the modern media landscape's unfiltered diversity, the uncritical reader is a valuable asset for an attacker. When false news is consumed on social media, assumed to be true and then distributed onwards, this contributes to increasing the scope of the attack and thus the damage and confusion that is the disinformation's purpose. Influence operations need not initially entail a concrete security threat, but in the long run they risk wearing down the institutions, trust and cohesion that are needed to confront a security threat.

Violent extremism

The extremist groups that thrive in the Swedish information environment also make use of the individual's emotional reactions. They frame the individual's frustration, anger, or uneasy sense of being disadvantaged within a simple and understandable context that in turn results in simple and understandable solutions. Of course, everyone has a right to proffer simplistic or erroneous claims within social discourse. The problems arise when extremist milieus (physical or virtual) generate individuals or groups who see coercion and violence, ranging from persecution of individuals to genocide, as the way forward. In those milieus that question or deny the equal value or legal rights of other people – while depicting themselves as righteous victims – it is often a short step to oppression and violence.

Violent extremism appears to be on the ascent in Sweden. This especially applies to the Islamist and the extreme right milieus. The tendency towards violence is found both at the level of individuals, so-called lone perpetrators, and groups. In this, developments in Sweden track with broader trends in Europe and globally.

Domestic and foreign networks

Violent extremist groups thus share the greater part of their worldview with broader extremist milieus in Sweden that refrain from advocating violence and thereby stay within the boundaries of the law. It is worth mentioning that the violent extremist Islamist milieu also shares central perspectives on the individual and society with another form of violent extremism, honour-related violence and oppression - despite the fact that the latter is not necessarily directly connected to either Islam or Islamic extremism. The concept of honour-related violence and oppression, as outlined by the government, includes phenomena such as coercive discrimination, physical abuse and even murder of individuals for the purported purpose of protecting a collective. Female circumcision, virginity checks, forced marriages and other forms of gender-based discrimination occur and comprise ways to preserve the collective's honour and uniqueness. It is done at the expense of the liberties and rights of the individual and constitutes a challenge to the principles of the rule of law.

Violent left-wing extremism appears to have lost much of its momentum in the last decade. It nevertheless remains active and finds itself, according to some observers, in a kind of activistic interplay with right-wing extremism: when right-wing extremism is more visible, the activities of left-wing violent extremists increase. A similar relationship is also found between the violent Islamist and right-wing extremist milieus. Violent left-wing extremists now present themselves as anti-fascist, using a broad definition of what fascism includes, but almost without exception consider their enemies to include the state, government authorities and the current social order. In addition, they have an expanded focus on, among other things, animal rights issues and environmental activism, which appears to increase the potential for violence around these issues.

Violent groupings are also found in complex international networks, with contacts that, thanks to technological progress, have become both faster and more difficult to monitor. The networks facilitate information-sharing, inspiration and exchange of ideas, as well as coordination of tactical initiatives and strategic efforts. For example, a part of the right-wing extremist movement is in contact with an emerging movement in the USA beholden to accelerationism – the idea that spectacular violent acts can hasten the unavoidable collapse of democratic society. Others parts are in contact with, among others, the ultra-nationalistic Russian Imperial Movement and its paramilitary branch, the Imperial Legion, which has fought on the Russian side in Donbass, Ukraine, and in Syria and Libya. The two Swedes behind the bombings in Gothenburg in 2016 had earlier that year undergone a paramilitary training programme in a training camp run by the Imperial Legion, outside Saint Petersburg.

At the same time, violent Islamists in Sweden have established contacts with, for example, the Islamic State and al-Qaida, both of which use violence for the purpose of establishing a worldwide caliphate. These contacts have resulted in violent acts within the framework of the war in Syria, the involvement of Swedish citizens in terrorist acts in Europe, as well as the planning and execution of terrorist attacks in Sweden. Additionally, violent Islamism and right-wing extremism are both connected to different forms of criminal activity.

Complex relations and common denominators

One could make it easy for oneself by saying that what is described above is simply an overview of the various components of the asymmetric threats. For each of these components there is a government ministry or agency that has been assigned management responsibility. Each agency, in turn, has its own mandate, its own manuals and its own action plans. What makes such an approach unsustainable is that the components can only be properly understood as an integrated whole.

The ways in which government ministries and agencies choose to handle each individual component can have system-wide repercussions. An inadequately holistic perspective and inadequate coordination can themselves be security-threatening factors. For example, how should one deal with domestic violent extremists using fake news produced by foreign intelligence agencies to influence opinion in the public forum? What should one do when a problem such as the democracy-threatening effects of honour-related violence and oppression are comprised of so many components that they are in practice divided between at least a half-dozen ministries and agencies? What does one do when two values – democracy and security – come into conflict?

There are thus good reasons to move towards a more holistic perspective in research and analysis, as well as in practical approaches to this problem set. The various groupings, networks and phenomena interact, impact and influence each other within a contiguous system. Analysis of individual components can never capture the dynamics of the system as a whole, pinpoint actions may impact some components while leaving the system intact.

Why a new concept?

The concept of democratic security describes a primarily social science research approach within FOI that views antagonistic threats against democratic rights and freedoms and against the principles of the rule of law as an integrated problem space. This holistic perspective has led to two main points of departure. First, that an analysis of the components of a threat must relate to totality of the problem space. Second, that efforts to deal with a threat must be based on and contribute to the democratic values one intends to protect.

Within security studies, the broadening of the security concept has been underway for quite some time. Traditionally narrow perceptions of security as only relating to the preservation of the state's monopoly on violence and the application of military power in the international arena have been widened. This has occurred, for example, by taking into account the impact of structural and discursive factors, and by considering the situation of vulnerable groups and their perspectives on conflict.

The battles over scientific methodology have been long and hard-fought, however. Modernist positivism, centering on measurable facts and objective truths, has come up against the subjective and relativistic perspectives of postmodern constructivism. In a meta-analysis of research theories, however, sociologist John R. Hall has shown that the firewalls that have been established between fact- and value-based methods in the social sciences are actually fictitious. There are good grounds for integrating seemingly conflicting methods and explanatory models. Thus, there is also a good foundation for creating a broader and deeper understanding of the many dimensions of the challenges.

A broader understanding of security revolves around not only what is threatened and by whom, but also how and why the threat arises, whether one can confront it before it arises, and the ways in which other threats are affected by measures taken. Complex problems require appropriate tools. Those who are responsible for confronting threats must be equipped with tools that can manage both depth and breadth. Our claim is that efforts to deal with the security of democratic society in ways that strengthen its resilience require more than the "top-down" responses of traditional security actors.

The Armed Forces' understanding and management of conflict dynamics during overseas, for example Mali and Afghanistan, have been improved by consciously applying gender perspectives to conflict analysis; not instead of, but as a complement to existing analyses and methods. Similarly, the capability of the Swedish Police to prevent violent confrontations has been reinforced by integrating insights from Social Identity Theory into the existing routines. This approach emerged following the extensive problems in dealing with the riots in Gothenburg in 2001, and led to the formation of Dialogue Police and the development of the Special Police Tactics concept. This shows that it is possible also organisations with extensive experience, solid knowledge and longstanding methods to advance and become more effective by adopting a broader approach and learning from new and seemingly peculiar methods.

The responsibility for protecting democracy and the rule of law requires active coordination and transparency towards the actors who build and safeguard a robust democracy; that is, civil society and, ultimately, the Swedish people. For example, neither social alienation, nor an inability to conduct source criticism, is in itself a security threat, but they are nonetheless recurring factors in democracy-threatening activities. This observation gives a central role in the protection of democracy to a greater range of actors that those government agencies responsible for surveillance and law enforcement. The ambition should be to prevent acute security issues. Democratic security, as a concept, creates the breadth needed to be able to understand and prevent the security-threatening activities of antagonists, as well as to predict and inhibit security-threatening consequences of the state and the government agencies' own responses to the challenge.

FURTHER READING

Strindberg, Anders, 2021, *Social Identity Theory and the Study of Terrorism and Violent Extremism,* FOI-R--5062--SE.

MSB, 2014, *Att värna den demokratiska rättsstaten,* MSB706 – maj 2014, ISBN 978-91-7383-455-1.

4. Robust decisions for managing a changed climate

Christoffer Wedebrand, Karin Mossberg Sonnek and Per Wikman-Svahn

Since 2007, when the Swedish Commission on Climate and Vulnerability presented its report, Sweden's municipalities, county administrations and authorities have begun to work in earnest on climate change adaptation. The work is urgent, not least because the cost of neglecting to adapt society will be calculated in the billions. But, at the same time, the effort is made more difficult by the great uncertainties associated with climate change and its future impacts. Below, we demonstrate how these uncertainties complicate decisions on preventive measures. We also provide a proposal for managing the problems – the proposal is closely related to methods developed by FOA's researchers during the Cold War.

Climate change leads to both certain and uncertain natural events

Thanks to research, we have good knowledge that greenhouse gas emissions change the climate. We also know that a changed climate increases the risk of different kinds of natural events, such as flooding and erosion, due to rising sea levels. Sweden is also exposed to these risks; for example sea level rise threatens residential areas as well as important activities and infrastructure in our coastal communities. Unfortunately, there is inertia in the system, which means that even if all the countries in the world radically reduce their emissions, the climate will still continue to change. It is thus necessary to implement measures to reduce climate's influence on society, which is called climate change adaptation.

But, at the same time we know that the climate is changing, we know less about how quickly it will happen and how it will affect our communities in the future. Several factors contribute to this uncertainty. A decisive factor is that we do not know how our communities are going to develop with time. Therefore we also do not know what the quantities of greenhouse gas emissions will be. In addition, it is difficult to determine how the climate is going to be affected by specific concentrations of greenhouse gases in the atmosphere. Not least, it is difficult to know what effects will occur at the local level as a result of a globally changing climate. Taken together, circumstances such as these make up a cascade of uncertainty that makes it impossible to predict the future in detail.

It can therefore be said that climate change and its effects in the form of natural events are both certain and uncertain: we know that the climate is changing and that it is going to affect us, but we do not know how nor to what extent. Consequently, it is also difficult to determine just which measures should be implemented to deal with the impacts of a changed climate.

A concrete example is the state of knowledge about rising sea levels. Scientific research has shown that sea level is rising and that it's doing so at an increasingly rapid rate. Research has also clarified what the most important causes are, namely, that warmer water leads to increased sea volume and melting ice on land increases the total amount of water. It is more difficult, however, to determine how much and how quickly the oceans are going to rise.

Different organisations' predictions of future sea level rise thus contain relatively wide margins. For example, the UN's Intergovernmental Panel on Climate Change (IPCC) indicates, in its 2019 report, that the average global sea level, compared to the reference period, 1986–2005, may rise 0.29–0.59 metres by 2100, in a low-emissions scenario, and by 0.61–1.10 metres in a high-emissions scenario.

The IPCC states, however, that there is a 17 per cent probability that the sea will rise higher than the highest levels indicated by the intervals in both emissions scenarios. In an analogy to playing dice, this is equivalent to the probability of throwing a six in one cast. Not especially improbable, in other words.

Other organisations have tried to estimate the probability distributions for more extreme sea level rise. Among these, the report from the USA's much-discussed 2017 National Climate Assessment can be mentioned. A scenario with high emissions of greenhouse gases indicates a possible sea level rise of 2.5 metres by 2100. Granted, the probability that the scenario will occur is certainly less than one per cent, but it is nevertheless considered possible. The report also describes scenarios up to 2200 that suggest the oceans will continue to rise even after 2100 and that much higher levels are possible.

In simple terms, sea level rise can just as much be expected to be rather small as extremely large. This uncertainty entails, or at least should entail, a major headache for those who work to protect our communities from the negative effects of climate change. Especially since the long-term costs of the sea level rise's consequences for infrastructure, residential areas and cultural values in coastal communities may eventually be calculated in billions.

Is it even meaningful to try to implement preventive measures when we do not know whether the ocean will rise 0.3 or 2.5 metres by 2100? Yes, we certainly think so!

Robust decision-support methods for managing an uncertain future

Given the major uncertainties in how quickly and by how much sea level will rise, one realises that adaptation measures that are chosen on the basis of just one likely future scenario risks being wrong. At the same time, it can be considered unnecessary, just to be on the safe side, to prepare oneself for the worst imaginable scenario, since the probability that it will occur is so small. In that case, we would have made unnecessary investments, perhaps at the expense of other important areas.

An alternative can be to use so-called robust decision-support methods. These methods involve finding robust measures, that is, measures that work fairly well regardless of how the future turns out. For this reason, these may come in handy for dealing with the effects of climate change. There are several different robust decision-support methods, but as a rule they build on the same principles, namely;

- embracing uncertainties;
- beginning with the decision situations;
- finding robust measures.

Embracing the uncertainties means, simply speaking, to not close one's eyes to the prevailing uncertainties about the future. To the contrary, this principle underlines the importance of relating to the actual uncertainties; for example, by not being content with the IPCC's interval for sea level rise, which only includes 67 per cent of the possible outcomes. The prevailing uncertainties should also be clearly reflected in the decision-support material that is used. Embracing the uncertainties also means taking into account the risk of extreme outcomes, even if these have a low probability.

Beginning with the decision situations is best understood in contrast to the more common approach, which is to first try to predict what is going to happen, by for example generating the most likely development, or the supposedly worst course of events. In contrast to this, the principle here is to first assess which vulnerabilities the community has, possible measures and their availability, and how long the measures may be effective. Only then is an in-depth analysis of the uncertainties undertaken, with a focus on the relevant areas.

Finally, the principle of finding robust measures involves, searching after those that work well for a large number of uncertain outcomes. The whole point of the first two principles can be said to promote the search for such robust measures. Static strategies involve deciding on the measures beforehand. The measures are then put in place once and for all and are intended to work well in many different imaginable future scenarios. The flexible strategies, on the other hand, do not consist of pre-selected measures. Instead, the strategy consists of several alternatives that are adapted depending on how the future actually develops. To illustrate, a static strategy could be to build high levees around an area today in order to protect against sea level rise, while a flexible strategy could be to raise the street levels and the floors inside the buildings at the same pace as the sea rises.

Within the frame of the research programme, *Robust decisions to manage climate risks in Sweden*, financed by the Swedish Civil Contingencies Agency – MSB, researchers at FOI, KTH and Lund University investigated the extent to which the three principles for robust decision-making are used in physical planning contexts in Sweden. The results indicate that they are not applied to any great extent and that it is most common to plan on the basis of a line above which it is considered safe to build. The line is most often determined through a worst-case scenario for the most likely sea level rise by 2100 and is independent of the planning situation. It is worth noting that the line does not take into account any continued rise in sea level beyond the turn of the century.

The research programme also investigated the possibility of using the three principles for robust decision-making in the physical planning of three municipalities along the coast. The results show that there is much to be gained by introducing a new approach to physical planning, but also that there are many obstacles. Among other things, current legislation on detailed development plans impedes the possibilities for placing demands on future (flexible) measures that could be applied when sea level has reached a particular level.

Managing uncertainty within the former total defence

Even if the use of robust decision-support methods can be considered to be a new way to manage uncertainty in today's work with climate adaptation, the three principles described above are not new in managing uncertainty within other areas. Similar principles were used in planning Sweden's former total defence. Researchers within the then Swedish National Defence Research Institute (FOA), one of the predecessors to FOI, proposed in a report, in 1994, a number of guiding principles "for those who work with planning under uncertainty or pursuing futures studies". The principles built on the researchers' own praxis and experience of planning within civil defence.

Similar to the principles outlined above, the FOA researchers meant that the future's uncertainties often has to be accepted and that this uncertainty should be highlighted. The researchers also pointed out that it does not always pay off to reduce the uncertainties. Whether or not it is meaningful must be determined, according to the researchers, against the background of the decisions that are going to be taken. The researchers also proposed a procedure that is very close to the principle of beginning with the decision situation, which they themselves call a bottom-up approach. In other words, do not start by formulating scenarios, but instead begin with an assessment of available resources and their incremental changes. Interestingly enough, the researchers also advocated the use of flexible measures, which they themselves called active measures, which are chosen continuously over time in the light of how the future unfolds.

Overall, we can ascertain that even if the specific threat that was being planned for differs, the approaches the FOA researchers used to deal with uncertainty in preparedness planning during the Cold War also remain relevant today. The same decision-support methods seem to be useful regardless of whether it is adaptation as a result of climate change, or other societal challenges, that is being dealt with.

FURTHER READING

Dreborg, K-H, Eriksson, E. A., Jeppsson, U. and Jungmar, M., 1994, *Planera för det okända? – Om hantering av osäkerhet.* Försvarets forskningsanstalt. FOA-R--94-00005-1.2--SE.

Wedebrand, Christoffer, 2020, *Planering under osäkerhet: Om att planera för det okända inom krisberedskapen, totalförsvaret och andra områden.* FOI-R--4972--SE.

Wikman-Svahn, Per, 2016, *Principer för robusta beslut inför osäkra klimatförändringar.* Kungliga tekniska högskolan. ISSN 1402-7615. TRITA-IM 2016:02.

5. The threats of the future – Do we see them coming?

On Sweden's arms race into a cyberfuture with linguistic challenges

Vidar Hedtjärn Swaling and Jenny Ingemarsdotter

The society of the future and new threat scenarios are being formed in the digital arena. But instead of looking outwards at specific types of cyber threat, we look inwards and observe how Sweden's zeal to be world's best in digitalisation can create security risks through underestimating vulnerabilities. In this context, we also illuminate a type of challenge that Sweden shares with the rest of the (cyber) world, a challenge for our imagination: How can the threats of the future be made comprehensible in a world of increasingly integrated intelligent machines? How much longer will the simple metaphors that permeate our language persevere, and how can Sweden equip itself for a future where the threats are ubiquitous and pervasive?

The allure of the digitalised society

The digital transformation is welcome in Sweden. Sweden wants to be on the leading edge: a modern country with smart cities, a country on the front lines. At the same time, the combination of technological optimism and arms race mentality have created flaws in the requirements when new technology is to be introduced. As the visions race to win the future, things that seem heavy and down to earth, such as infrastructure and security, have a hard time receiving attention. Digitalisation has in many cases become an end in itself, rather than a means.

The speed of development is fanned by more or less aggressive technology campaigns. But the notion of Stockholm, for example, as the world's smartest city is not accompanied by an idea of how it can become secure to the same degree. Those strategies and visions that emphasise digitalisation's opportunities instead warn that development is going slower in Sweden than in other countries. Neglecting the foundation, however, can result in services running counter to their purposes, for example by creating increased costs, inefficiencies and frustration, rather than utility, as well as by building vulnerabilities and security problems into the new systems.

Thus, today there are digitalisation projects that have become resource-consuming black holes, that in addition have created an administrative burden for both personnel and citizens. Unfortunately, there is nothing to indicate that this will straighten itself out with time. To the contrary, one can imagine that lock-in effects emerge, as problems become so complex that they become difficult to overview and extricate oneself from. The concept of the *internet of things* drives this development further, since in principle it can gather everything around us – from toothbrushes and vacuum cleaners to elevators and drawbridges – and connect it together.

Add to this threats. They can arrive in the form of automated but intelligent attacks against our societally critical systems or against our democratic processes. But when one discusses threats and digitalisation, there is yet another level of problem: the risk of not even being able to understand what constitutes a threat, or how it should be described.

What happens when language is no longer adequate?

Threats are abstract in nature, at least in the sense that they refer to something that has not happened yet. To understand threats, one thus depends on language's ability to capture and convey phenomena that are supposed to be dangerous in some way, sometime. But what happens when new technology and new habits outrun our familiar concepts and categories?

An insight of modern philosophy of language is that our concepts are not disconnected from reality, but on the contrary are inextricably linked to how they are used. Concepts are not abstract entities deployed *about* actions, about methods, *about* habits and conventions, but are a part of them all. The connection between language and the everyday life it appears in is thus not fortuitous, but *necessary.* Does this mean that the difference one sees between vision and praxis could lead to confusing and misleading speech?

An example of a threat that is hard to explain originates in the current convergence between the cyber and the physical worlds. Machines and processes have been controlled by computers for more than half a century. Originally, this involved tailor-made systems with highly specific tasks. But today almost anything at all, in principle, can be connected to ordinary computer equipment, locally or on internet, for communicating, controlling and surveillance. That a system is cyber-physical means that it has become unclear where one begins and the other ends, a vagueness that grows when everything can be hooked up and when the connection moves ever further into cyberspace. What will be a gadget in the future? More precisely, what is cyber and what is physical when these two worlds begin to presume, require, or are premised upon, each other? The emerging *internet of things* does not merely involve increased connectivity, but a transformed existence, with intelligent systems that are ubiquitous and pervasive. Our language, and therefore our thinking, are at the same time characterised by fundamental spatial metaphors.

Three digital change paradigms

We have identified three sociotechnical megatrends, or change paradigms, which are well on their way to changing the very foundation of our metaphors and, by extension, our way of understanding the world.

- Cyber/physical – things are connected.
- Data/individual – data drives society.
- Human/machine – computers become intelligent.

That things are connected, perhaps never to be disconnected, as in the *internet of things*, changes our understanding of what a thing is and the relations of things to each other. Similarly, *Big Data*, and data as the new fuel for society, are expanding and relaxing the limits of the individual. Progress in artificial intelligence (AI) in turn challenges the division between humans and machine. The starting point is that phenomena that previously were separate have increasingly begun to overlap and merge, at the same time as the three change paradigms together drive and create new digital threats and vulnerabilities. In the intersection between these paradigms, an intelligent entity can emerge that is vaguely represented in the physical world, with enormous potential to influence it.

At the same time as many future threats are going to be developed within these change paradigms and in the interfaces between them, there are great gains to be made by those who understand how to take advantage of technology's new possibilities. There are also hopes that new smart technology will be able to solve the great challenges of our time: the climate, energy needs and welfare. In Sweden, not least, grand visions have been formulated where digitalisation is the solution to the challenges of the future. But do we always understand what we are up to?

In a country that has based its self-image on the notion of progress, which basically means seeing oneself as continuously moving forward, the work on security and risk analysis can be perceived as showstoppers. At the same time, the issue of the threats of the future is right before us. But an adequate threat perception is not something we can acquire in hindsight. It is built up slowly, as a part of technological development, and it is underway now.

FURTHER READING

Ingemarsdotter, J., Eidenskog, D. and Swaling, V. H., 2020, *Vilse i lasagnen? En upptäcktsfärd i den svenska digitaliseringens mångbottnade problemstruktur.* FOI-R--4814--SE.

Stenlund, S., 1990, *Language and Philosophical Problems.* Cornwall: T J Press (Padstow) Ltd.

Lakoff, G. and Johnson, M., 1980, *Metaphors We Live By.* Chicago: The University of Chicago Press.

6. AI and influence operations in social media

Fredrik Johansson, Magnus Rosell and David Gustafsson

Influence operations have been playing an ever increasing role in social media during the last decade. This involves conscious fabrication and spreading of false or misleading information intended to influence a target group. Influence operations can be conducted by any actors, from state actors with political motives to individual actors who act from economic interest. Not least in connection with referendums, researchers and employees from social media platforms have been able to identify how so-called troll factories systematically use large numbers of false user accounts for the purpose of spreading fake comments and false or angled news. Influence operations occur, though, more or less continuously. However, it is more difficult to trace their origin to a specific source, which makes them a popular tool for attempting to influence, with little risk of discovery or reprisals, a target group's behaviour or views on a particular issue.

The rapid development of artificial intelligence (AI) has led to a dramatic improvement in the quality of automatically generated text, that is, text that is created without human interaction. In many instances, it is difficult for people to distinguish between genuine and automatically generated text, even when it is clear in advance that a text may potentially be a generated one. Similar techniques can be used to generate and manipulate photos, video and voice in such a believable way that it is difficult for the human brain to tell them apart from the real thing. This can have a strong impact on our digital information society, as in the near future we risk being flooded by enormous amounts of automatically generated content, produced at minimal cost and with an authenticity that we cannot verify with our own senses. This risks fanning a societal development where truth becomes secondary and subjective opinion primary. Addressing this social challenge requires a number of measures where AI technology for detecting automatically generated content has an important role to play, but is nevertheless insufficient. An increased awareness of the existence of the problem is also an important part of the defence against influence operations, which is itself an important motivation for writing this article.

False information and influence operations in social media

That false information is created and spread in social media is by no means only a future threat, but something that is happening already today. Reviews of products and services is one area where there has long been an economic incentive to enlist people to write fabricated reviews, either to promote one's own product or smear competitors. Several studies have shown that this is a commonly occurring phenomenon on services such as Yelp and Amazon. The same also applies to false news. Numerous reports have highlighted how a large number of individuals in eastern European countries have created fabricated news about everything from celebrities and health trends to American politics. These false news are spread with attention-grabbing headlines on social media platforms such as Facebook and attract clicks that generate cash in the form of advertising income.

This has a negative impact on trust in the digital information in social media and on the web. Unfortunately, it doesn't end there. Large-scale political influence campaigns are also carried out in a digital milieux. This was revealed, for example, during the US debate on net neutrality, in 2017. Millions of automatically generated comments that criticised that internet providers did not have permission to control the flow of information on internet were created using simple templates. The purpose was probably to influence decision-makers by delivering a skewed or strongly amplified impression of public opinion. Another illustration is the attempts by various state actors to influence opinion or create divisiveness in other countries, where the so-called troll factory in Saint Petersburg is a well-known example. Figures from leaked documents and journalists' surveys show that every month major funds are spent by Russian elements to create and spread fictive content intended to appear as if it is ordinary user commentary. Russia, however, is far from being alone in engaging in this kind of activity.

The threat from automatically generated text content

Creating and spreading false information has until now been relatively expensive, since it requires manual inputs, which has likely contributed to limiting the problem. Applications of AI models that have been trained using huge quantities of text data and capable of generating new texts of good quality are already available. These are commonly called pre-trained language models. Training language models, however, can require advanced resources, but once they are in place it costs almost nothing to generate new texts of good quality.

This means that before long we risk being flooded by computer-generated false news and fictive commentary in social media. The two greatest reasons why this hasn't already happened are probably that, previously, it was difficult to control the models to generate texts that fit one's own agenda and, in addition, "keep to the thread" throughout a longer quantity of text. These obstacles are now being overcome. We believe that it is just a matter of time before pre-trained language models that are easy to control are widely available, even for such minor languages as Swedish.

Texts generated by language models are difficult, language-wise, to distinguish from those written by a person. The sceptical reader might object that persons schooled in source criticism can easily realise that the information in a text cannot be trusted just because it is well written and that therefore it should not have any influence on them. Claims must be fact-checked and verified against other, independent sources. An aggravating circumstance is that journalists pressed for time occasionally pick up news from social media, write articles based on them, and refrain from checking their facts. On the other hand, playing it safe and merely trusting information from news media of high journalistic standard and a well-established tradition of fact checking, however, is not necessarily a completely reliable strategy either. There are examples of verified accounts belonging to highly reputable actors, the Associated Press, among others, who have been hacked and used to spread false news with rapid distribution, and which have led to major but temporary economic consequences. All in all, this means that no single factor is completely reliable in assessing the credibility of a text, which makes the quality of the text just one of several factors that are consciously or subconsciously weighed when doing so.

The threat from automatically generated audio, images and video

An additional precaution would be to only trust information that can be verified through one's own senses. Knowing that it is possible to make an e-mail message appear to have been sent from another address than the original one, or that the account has been hijacked, can lead an aware user to trust, in the digital world, only those voice or video calls where the other party can be heard or seen. The problem, once again, is malevolent application of modern AI technology. There are already examples of how this type of technology is used by fraudsters to get employees in a company to conduct transfers to external accounts. Progress within so-called voice cloning has been so rapid that a recording of someone's voice only a few minutes long is enough to generate new speech of good quality and with unlimited content that sounds as if it was said by the person whose voice was cloned.

Progress in the image and video area has also been so great that it is now possible to generate completely synthetic high-resolution facial images of persons who do not exist, or to manipulate such attributes as sex, hair colour and age in a credible manner. It is even possible to replace the faces of persons in films, so called *deep fakes*, or simply create video clips, almost in real time, where both real persons and synthetically generated avatars can be made to speak and move in the same way as a real person. So far, video clips can only be generated with relatively limited resolution, but we believe that it is just a matter of time before almost anyone will be able to produce high-resolution video sequences of good quality that are very difficult to distinguish from authentic video films.

A consequence of this development is that it is becoming increasingly difficult to use our human senses to judge whether digital information, either as text, sound, image, or video, is correct or not. Given this description of our possibilities to assess digital information, it is easy to be pessimistic. Our society is nevertheless much more digital now, so that if we returned to relying only on our own senses we would lose many of the advantages and opportunities the connected information society actually offers.

AI technology as a defence against automatically generated or manipulated content?

A defence against those threats that our open and democratically connected information society faces requires educational efforts in a number of areas. This can involve source criticism and knowledge about what can actually be achieved in terms of generating or manipulating text, sound, images and video with modern AI technology.

Increased awareness and knowledge of source criticism are not enough, however. On the basis of our technological perspective, technical development and AI research are not only the reason for the existence of the threat but also the opportunity to find a solution to the problem. At FOI, we are conducting research around the possibilities of using machine learning to develop methods that can support people in determining whether material is authentic or not. For example, whether a text has been written by a person or a computer, whether a photo of a person was taken in the real world or generated with the aid of AI, or whether the sound or images in a video sequence have been manipulated or not. These are research areas that have recently been receiving increased interest and quickly demonstrated great potential. A challenge is to make the detection methods that are successful in well-controlled experiments to work on data that deviates from what the methods have been trained on, while being sufficiently robust and scalable to work well in practice. Factors such as dealing with data that can have other characteristics than those used for training, for example various degrees of compression, also negatively affect the result. In addition, new and improved methods for generating and manipulating data are continuously being developed. AI-based detection methods can never be our only defence against malicious actors, although they are an important tool. We mean that trust in this type of technology requires detection algorithms that not only are highly accurate but also that the resulting models can be made transparent, so that human users can understand what the assessments are based on. This applies not least, to whether the technology will be used as evidence, for example in police investigations or lawsuits.

Social media companies also have an important role in this. Beyond having access to content, they also have information on IP addresses and distribution patterns that can be used in for example identifying suspects or coordinated accounts. In the beginning of 2020, Facebook issued a ban on misleading manipulated pictures and videos on its platform. Twitter has on several occasions shut down accounts and published lists of accounts that they judged were involved in different forms of state-actor-supported influence operations. These are praiseworthy initiatives by private companies, but there is also a need for clearer and updated legislation in this area.

Different kinds of authentication mechanisms can in future help in various ways to verify the authenticity or integrity of digital media. An example is the use of block chain technology similar to that used in digital cryptocurrencies or various forms of digital signatures that are destroyed if the media is in any way corrupted. There is probably no universal solution, but there is good hope that through the application of a number of technical solutions, education and updated legislation, the implementation of influence operations can be thwarted.

FURTHER READING

Johansson, F., Horndahl, A., Stiff, H. and Garcia Lozano, M., 2020, *Data Synthesis using generative models.* FOI-R--5041--SE.

Johansson, F., Horndahl, A., Lilja, H., Garcia Lozano, M., Lundmark, L., Rosell, M. and Stiff, H., 2021, *Detection of fabricated media.* FOI-R--5732--SE.

7. Swarming drones – a realistic future threat?

Martin Hagström, Lars Forssell and Niclas Stensbäck

The development of small drones is proceeding at a blistering speed and the consumer market offers civilian systems that continue to become cheaper, and equipped with ever more autonomous functions that support their piloting. Is the battlefield of the future going to be dominated by swarms of armed drones? And, if so, are there any limitations to this threat?

Small, armed drones using advanced image processing and cooperation to defeat an enemy has long been presented as a threat that is going to revolutionise warfare. In the film *Slaughterbots*, produced by the organisation *Future of Life Institute*, a fictional company has developed drones, supposedly as a military weapon, which are then used with social media to track and kill both political opponents and young protesters. The film was released in 2017 to bolster debate on artificial intelligence (AI) in weapon systems and gained relatively widespread attention. Other examples of AI's running amok are the classic film *2001: A Space Odyssey*, from 1968, and *Stealth*, from 2005.

However, how realistic are these visions of the future, with advanced target-seeking drones that can both recognise their targets and act against them? What is the current state of armed drone development? In addition, what military threat will the futures armed swarms pose?

For many years now, it has been possible to purchase over-the-counter unmanned aerial vehicles (UAV's), popularly known as drones, and to build them using readily available components. Drones as weapons of simple design have been used for many years by, among others, non-state actors, in the conflicts in Libya and Syria, and in an attempt to assassinate Venezuela's President Nicolás Maduro. Companies from several countries market UAV's with different weapon payloads. For example, Uvision, an Israeli company, has developed a product line of loitering munitions, the smallest of which weigh only 1.8 kg, that are designed to be used for both reconnaissance and combat.

Today, many private citizens are flying drones with, or have seen drones with, the ability to follow a person automatically while avoiding collisions with trees (e.g. Skydio 2). Although their degree of autonomy has been developed over a long time, these drones nevertheless face a number of fundamental limitations that can be expected to constrain the swarming threat.

Limitations of the platform

The fundamental factors that limit the effects of a swarm of drones most are range, efficacy, communications and navigation, as well as the ability to adapt to new conditions. In addition, a system that will be used in military context must withstand a hostile environment while at the same time solving complex tasks.

The flight time of drones are limited, and although battery storage capacity has increased markedly during the last decade, flight time can still be expected to be a limiting factor in the future. This means that the drones need to be transported to their area of operations, in order to carry out their mission. Drones that function as small helicopters with several rotors are naturally inefficient platforms. Such a multicopter's ability to rise vertically and manoeuvre comes at the price of much higher energy consumption compared to flying with a fixed-wing aircraft.

All aircraft have a fundamental conflict between range and payload capacity. This is especially true for small drones that can carry only a very limited load. For an armed drone, weapons are the primary payload. Since long ranges limit the payload that can be transported, neither heavy sensors nor explosives can be carried.

Weather resistance is a concept used to describe how robust a system is against natural disturbances. For a smaller drone, wind and rains will be limiting factors. In a strong wind, drones may simply not be able to fly and if it rains their cameras quickly become unusable, something that anyone who wears glasses has no doubt noticed on a rainy autumn day. Cold also affects drones, since it diminishes batteries' electrical output. Most small drones available today are fair-weather systems. Building a weatherable drone is not only associated with higher costs, it also involves the above trade-offs between range and sensor performance.

Navigation and communication

To be able to cooperate in swarms, drones need to navigate, to know where they are, and communicate with each other. The space available in smaller drones for physical communication components is going to be limited, such as antennas for satellite navigation (GNSS). In environments where it is difficult to navigate, such as cities, it will be necessary to supplement navigation via GNSS with other techniques. In the near future, navigation based on terrain recognition will be possible and drones will not be as dependent on satellite signals. This is not problem free, however. The sensors are, in part, dependent on good conditions and in part, will need to manage changes to the local environment, from snowfall to fog and the environmental changes resulting from warfare.

To see and engage

For a drone to be able to engage a moving target, it needs to seek and follow the target. Thus, the drone needs a seeker function, which is simply a sensor that can seek and follow the drone's target. An area that is undergoing rapid development is on-board, high quality image processing. Progress is moving towards both smaller and more powerful processors, which are constructed specifically to use image-processing algorithms both quickly and with low power consumption. A future where it is possible for systems with both regular cameras and infrared sensors to detect and classify hostile target automatically and with a high degree of confidence is not improbable. However, countermeasures in the form of advanced camouflage are also going to be developed.

Drones have a very limited capacity for carrying warheads. In the film *Slaughterbots* a shaped charge warhead (or HEAT) is used. This is a warhead where the effect is directed and a penetrating material is shot at extremely high speed, faster than the bullet of any rifle. This is a technique, known since the Second World War, which is commonly used in modern warfare against tanks and other armoured targets. Large warheads of this type can pierce through metre-thick armour plates. When the size of the warhead is reduced, however, the effect is reduced relative to its weight. Shaped charges do not scale well, and it is difficult to build miniaturised charges that are suitable for small drones. In addition, the warhead is dependent on being close to the target when it detonates; a simple method of protection, perhaps not practical in all applications, is to merely set up a net around the target. Another way to arm a drone is to mount some form of ballistic weapon, for example a part of a firearm, and use the drone as a gun carrier. There are many examples where drones have been used in this way. How a drone-borne small-calibre weapon can attain the necessary precision and rate of fire to take out a military target in a cost-effective way is, on the other hand, not clear.

Swarming

The word swarm is borrowed from nature, where insects, birds, or fish, together exhibit a more complex behaviour than that of any single individual. Research on how emergent capabilities are generated by the collaboration of single individuals, such as insects, is still ongoing. For example, there are research projects where a single operator controls a set of vehicles by distributing tasks, and the decisions of the vehicles flight paths are solved locally. However, there are still many unanswered questions regarding how swarms can build robustness by being self-organising and adapt their behaviour to solve tasks together.

Challenges arise when a swarm's self-organizing algorithms (sometimes using machine-learning techniques) make it difficult to predict which "decisions" the resulting swarm will make in any given situation. Additionally, research within counter-AI is growing, to find ways of deceiving an autonomous system.

Swarms can be controlled via centralised or decentralised principles. In centralised control, a central node collects data and controls the task of the drones. This principle allows an operator to have better control over the swarm, but places higher demands on communication. It is also sensitive to external and internal interference. An example of centralised control is civilian air traffic control, where every aircraft has pre-approved flight plans and is led by an air traffic control system.

In decentralised control, every drone makes its own decisions, based on its own local understanding of the situation and the overall task. In a flock of birds, every bird strives to fly in approximately the same direction and speed, and each one avoids collisions when they notice that they have come too close to each other. These two rules are enough to coordinate a large number of birds. This type of solution is more robust against interference and can be adapted to a changing surrounding, but does not offer the operator the same control over the swarm's behaviour. Deciding which principle of controlling swarms is optimal in a given situation, centralised or decentralised or a combination of the two, is an open research question. Building autonomous drones that have the ability to generate flight paths and use sensors to detect and classify targets, in collaboration with each other, is a highly complex technical problem, which likely will be challenging to develop and implement.

Predictions of future swarms that are dispatched to find and engage enemies, often lack an important perspective when it comes to conducting warfare. The military utility of a technical system relies on, among other things, security and control capability. This means that the commander of an operation must have a good understanding in advance, of the effect the system has in time and space. It is not clear that the military utility of intelligent, autonomous swarms is going to justify the cost involved in developing such functions.

In the foreseeable future, small drones can be expected to continue to have limited range and endurance. They will also have difficulty acting in a hostile environment where an enemy can disrupt their communication and navigation capability. It is also not clear that small drones will have the capacity to form a threat against a protected military target. To give drones better range, effect and to make them more robust, they need to be larger and more capable. This means that the cost of a single drone will increase drastically and therefore the number of drones that make up a swarm can be expected to decrease. However, fleets of drones are already used today as terror weapons and against civilian or unprotected targets and can in that perspective continue to present a threat.

Our assessment is that for the foreseeable future, swarms of small-armed drones, because of their limitations, will not pose a decisive threat for military targets with modern equipment and protection. They are still relevant threats though, during asymmetric warfare or when used by terrorist organisations, which is well worth further research. The large swarms that are going to revolutionise war on the battlefield, however, remain science fiction and a future scenario rather than an actual threat.

FURTHER READING

Ekelhof, M. and Paoli, G. P., 2020, *Swarm Robotics: Technical and Operational Overview of the Next Generation of Autonomous Systems,* UNIDIR.

Schmuel, S., 2018, *The Coming Swarm Might Be Dead on Arrival,* https://warontherocks.com/2018/09/the-coming-swarm-might-be-dead-on-arrival/ (accessed 2021-01-13).

Scharre, P., 2014, *Robotics on the Battlefield Part II: The Coming Swarm,* Center for a New American Security.

8. Can laser weapons be a game changer in future conflicts?

Matts Björck, Markus Henriksson and Lars Sjökvist

When Theodore Maiman demonstrated the first laser, in 1960, many realised its possibilities as a weapon. Laser weapons are now starting to see the light of day, with some having already been used in the field in ongoing conflicts, and prototypes are being developed by numerous countries. It is easy to believe that laser weapons are going to be as powerful as the ray guns in science fiction movies, but will they really? Below is a description of how laser weapons can be used and what would happen if one met an enemy who used them.

A rapid precision weapon with an endless magazine

There are several reasons why most major military powers are developing laser weapons. First, the speed of light is about a million times faster than a rifle bullet. The target will not move during time the laser beam leaves the weapon until it reaches the target. Second, the laser beam can be focused to strike an area as small as a postage stamp from several kilometres away, which means that the most vulnerable part of the target can be selected with precision. Third, the absence of a projectile and explosives means that the risk for collateral damage is limited. Finally, today's lasers are powered by electricity. As long as electrical power is available the weapon can be fired, a capability that in military terms is known as having a deep magazine. A fully charged electric-car battery holds enough energy to fight several targets, while more powerful laser weapons require the output from several batteries connected in parallel.

Today's laser weapons use fibre lasers, which are categorised as solid-state lasers. High-powered fibre lasers are used in manufacturing, for laser cutting and welding. Fibre lasers use the electrical output of a large number of diode lasers to create beams that are absorbed in the fibre's core. The absorbed energy is used to create a new laser beam that can be focused much better than the beams from the diode lasers. Laser weapons consist not only of a laser. Camera technology is also required to follow the target as well as mechanisms and optics to direct the laser beam towards the intended point on the target. Additionally, an electrical system is required that can produce high output when the laser is to be used and a cooling system to deal with waste heat. Laser weapons also need to be integrated in a command and control system that, for example, designate targets.

When a laser beam strikes an object, part of the beam is reflected and the rest is absorbed, becoming heat. When a material is heated to high temperatures, its structural integrity is affected and external forces can break the target apart, and for example, a control fin on a missile can be broken off. If the material is further heated, it begins to melt and the laser burns a hole in the material. If the object contains explosives or fuel, the heating from the laser beam can ignite it. Since the effect is a result of heating the material, the laser needs to illuminate the same point on the target long enough, which may take up to several seconds.

Laser weapons then and now

The threat of nuclear-armed intercontinental ballistic missiles was a constant presence during the Cold War. The USA allocated major resources to develop aircraft-mounted laser weapons to strike missiles during their start sequences. Because the missiles were large, massive objects located at great distance from the laser weapon, extremely high laser output and complex optical systems were required. Impressive prototypes were demonstrated, but the technology was too complicated and costly to put into service.

Since 2000, the focus has instead shifted to using the precision and speed of laser weapons to shoot down small, fast and easily manoeuvrable objects. The types of targets with priority are drones, rockets and artillery grenades, which are difficult to defeat with conventional weapons. Laser weapons can also be used against boats and lighter vehicles. Today, laser weapons are primarily seen as defensive.

The most well-known laser weapon system at the moment is the US's demonstrator, LaWS (Laser Weapon System), with an output of 30 kilowatts. The system was installed in 2014 on the ship *USS Ponce* for testing and was subsequently approved for use in operations in the Persian Gulf until 2017, when the ship was decommissioned. LaWS was then installed on another ship and the laser upgraded to deliver higher output. The system has been demonstrated against such targets as grenades and small drones and boats.

China has demonstrated, at arms shows, a laser weapon called *Silent Hunter*, primarily designed to shoot down low-flying drones. Russia has announced, in official statements, that it has laser weapons, although details have not been revealed. Also other major countries in Europe, and others such as Israel and Turkey, have active laser weapons programmes. According to reports, Turkey succeeded in shooting down a drone in the war in Libya, using a laser weapon they have developed. The drone was Chinese-built and owned by the United Arab Emirates.

Laser weapons have a number of challenges and limitations

To be effective against fast targets, laser weapons need a high laser output, so that the target can be neutralised before it manages to wreak damage. The greatest challenge is to have enough time to take out the incoming projectiles before they reach the target, especially if several are approaching simultaneously. The laser weapon must then be able to switch targets and combat several threats in an extremely short time. For larger targets, such as cruise and ballistic missiles, longer effective range and higher laser output than what have been demonstrated thus far are required.

Absorption and atmospheric dispersion reduce the effect of a laser when it reaches the target. This means that the performance, among other things, diminishes in fog or low clouds. Optical turbulence in the atmosphere, the phenomenon that for example makes the air shimmer above a warm road in the summer, distributes the laser's effect over a larger area on the target, thus lengthening the time it takes to attain the effect at a larger distance, especially if the laser beam travels close to the ground. The effect of optical turbulence can be reduced by adapting the laser beam to the turbulence; this can be done for example with adaptive optics or advanced beam control technologies.

Another limitation of laser weapons is that there must be a clear line of sight between the weapon and the target. This means that it is not possible to strike targets beyond the horizon. For a person standing at sea level, the horizon is about five kilometres away. This can entail a fundamental range limitation, but naturally, this depends on how high the laser is located over the earth's surface. Line of sight is an even greater limitation in complex environments of buildings and trees.

What are the implications of confronting a force protected by laser weapons?

An invader of Sweden could use laser weapons as air protection, mounted on both ships and trucks, to protect shore landings and bridgeheads. The most powerful laser weapons that have been demonstrated to date would be able to strike down an incoming artillery grenade within a few seconds, with a maximum effective range of three to five kilometres. In principle, this means that an invader armed with laser weapons can prevent their bridgeheads being struck by artillery and grenade launchers. Laser weapons can also stop incoming missiles. In these cases, however, the detection distance may be shorter, so that it is not certain whether the laser weapon will succeed in destroying the missile. An exception is missiles with semi-active laser target seekers, such as Sweden's Robot 17, where the target seeker would be immediately destroyed by a high-powered laser, which would make the missile lose control.

Reconnaissance with drones and other flying platforms against attacking forces is also going to be highly difficult. Laser weapons can take out cameras at very great distances. Drones can be shot down quickly if they come within a few kilometres and are detected. How sensitive our advanced platforms, such as the JAS 39 Gripen, are against laser weapons is not known. At close range laser weapons will be able to damage all types of platforms.

How can the effect of laser weapons be reduced?

As in all military duels, this involves means and countermeasures. Since laser weapons require a few seconds to act, an obvious countermeasure is to give them less time. This can be achieved by using missiles that are faster, by launching from positions where a laser weapon attains a clear line of sight to the target as late as possible, or simply by shooting with several artillery pieces, so that the laser weapon cannot manage to oppose every projectile. Another possibility is to lengthen the time it takes for the laser to act against a projectile. This can be achieved by altering its surface so that more of the laser beam is reflected, which in turn implies that less of the laser's beam is absorbed and transformed into heat. Alternatively, more heat-resistant structures can be used, for example using thicker grenade casings or by improving heat-conducting characteristics.

Today, conventional weapons probably retain the advantage in battle. Artillery should be able to destroy laser weapons through rapid fire. In a conflict, however, a laser weapon would not be acting alone and the objects they protected would manage to act in other ways. Laser weapons are also still a young technology, where development can be expected to proceed faster than for conventional weapons. Therefore, platforms and weapons need to be continually developed further to reduce the effect of laser weapons so as not to become prematurely obsolete.

So far, laser weapons should be considered as defensive weapons for protection of ships or staging areas on land, which thereby enables operations in areas where the force does not have control over the surrounding territory. On the other hand, development of aircraft-based systems that can attack sensitive targets is underway, and in the future laser weapons can be offensive weapons against targets on the ground.

Will they be just like in the movies?

The picture that emerges is that laser weapons are not going to be as spectacular as those portrayed in science fiction movies. These are not weapons that are going to dominate. Laser weapons are nevertheless going to strongly affect the effectiveness of conventional weapons by providing high-precision close protection air defences. This means that much greater firepower is going to be needed to fight an enemy who has laser weapons, or that, alternatively, weapons are needed that are adapted to the characteristics of laser weapons.

further reading

Sjöqvist, L., 2017, *Laser för skydd av strategiska objekt t.ex. flygbas*,
FOI Memo 6139.

Hecht, J., 2018, *The ray guns are coming*, IEEE Spectr. 55, 24–50.

9. Space is a warfighting domain

Sandra Lindström and Kristofer Hallgren

Future wars will play out in, through and against space. This is a relatively new reality with consequences for all of society, including our defence capability. When re-establishing the Swedish total defence it is essential to coordinate national civil and military space activities. There needs to be a better awareness and knowledge on the international developments within the space domain among Swedish authorities and decision-makers in order for them to efficiently support the establishment of a total defence.

This article describes the ongoing arms race and how space has transformed into a warfighting domain. It is notable that at the same time as society's security and military capabilities are becoming more dependent on satellite services, there are countries conducting tests of anti-satellite (ASAT) capabilities. A future conflict is going to involve the space domain. Therefore, we propose that Sweden develops a contingency plan to deal with conflicts, crises and warfare in space.

There is an arms race within the space domain

The space domain has changed dramatically in the last few years. Several major space nations recognises space as an operational domain. Space used to be a domain that supported military capabilities in other domains, but now space is seen as a domain like any other. There is an ongoing arms race within the space domain. Weapons are being developed and tested against satellites, with a hitherto unseen public openness and rhetoric. As the strategic advantages of ASAT weapons becomes apparent, more actors are striving to develop their own ASAT capabilities.

Ever since the first satellites were launched, space has been militarised. After the Cold War, as a result of rapid technological development and proliferation of space technology more nations began to use satellite services. Space was considered free from conflict and warfare. Today, however, several nations acknowledge space as a warfighting domain. Military doctrines for space operations have been developed and military organisations have been established to manage this development. Conflicts in space includes everything from interference of satellite services, disabling satellites to kinetically destroying satellites. The boundaries between what would be seen as an act of war and acceptable behaviour are unclear. For example, deliberate interference of satellites and cyber-attacks are occurring on a regular basis. Satellites that can be used for both civilian and military purposes, as rendezvous and proximity operation satellites, contributes to more tension between countries. Satellites with the ability of precision manoeuvring can approach other satellites, which can be mistaken for military threats, especially in the absence of transparency about their intentions.

Similar to the situation during the Cold War, there is an ongoing arms race within the space domain, which should not be confused with an arms race in outer space. This arms race primarily involves different types of counterspace weapons and is less about weapons intended to be placed in outer space. Information about new counterspace capabilities are commonly made public. Tests of ASAT weapons are nothing new and were regularly conducted by the USA and the Soviet Union until the end of the Cold War. After decades of relative calm, tests are once again being conducted. The difference, compared to the Cold War era, is that there are more nations conducting tests and significantly more actors, and satellites in orbit in risk of being collaterally damaged. Some even speak of a shift towards a normalising of testing and the use of ASAT weapons. The latest destructive ASAT weapon test was conducted in 2019, when India destroyed one of its own satellites in low earth orbit. The test resulted in relatively little space debris, most of it re-entered the atmosphere within a year. Reactions against the test were not as strong as one might have expected, but discussions about a ban on destructive testing have once again come into focus. It is worth noting, however, that most of the known weapons being developed today are intended to disrupt or interfere with the use of satellite services, rather than destroying satellites.

A conflict in space could quickly escalate to a conflict on the ground, and vice versa. Some nations consider that an attack against their satellites is equivalent to an attack on the state itself and refers to the UN Charter on the right to self-defence. This is based on the assessment that society and national security are critically dependent on satellites. A conflict on the ground could quickly escalate to involve direct actions against satellites. It is therefore highly likely that future conflicts are going to involve the space domain with a negative effect on satellites and satellite services in ways than we have not seen so far.

Sweden is dependent on space

Our society is dependent on the provision of satellite services to the right place at the right time. The government also believes that the societal benefit shall be central when carrying out Swedish space activities. Satellites are necessary for monitoring climate and environmental changes on earth. They are also essential for managing and limiting the consequences of natural disasters. Satellite information contributes to global transparency and thus adds to stability in security policy, because various actors become aware of activities occurring globally. Transportation becomes safer and more secure because it is controlled and monitored with the aid of satellites. They are also an invaluable resource, for example, in the work of the police and emergency services. Our electricity grid would not function without time references from satellites. For stock exchanges and banks as well as trading companies, exact time signals from satellites are essential for their business. These are only a few examples of how society utilises satellite services daily.

The use of satellite services is not always obvious for an end-user since the satellite information is refined in several steps. This means that it is sometimes difficult to know if a societal function is dependent on information that is delivered by satellites or not. There is probably both intentional and unintentional dependence on satellite services, which makes it difficult to identify vulnerabilities in critical infrastructure and important societal functions. In addition, some vulnerabilities can probably be accepted to varying degrees dependent on whether they arise in peacetime, during crisis or war. This assumes, however, that the vulnerabilities are known and that the risks are accepted.

Satellites and the services they deliver can be affected, interfered with or periodically disappear completely because of natural phenomena or malicious actors, with both direct and indirect consequences for society as a result. An indirect consequence is when satellites are owned by parties with interests that diverge from those of the Swedish society. When we purchase satellite services from a commercial actor, we can never be completely certain, that in the event of a crisis or conflict in peacetime and especially not in wartime, that those services still are delivered. Commercial actors are increasing in number and they offer numerous attractive services based on satellite information and hence our dependence on satellite information is growing.

Satellite services provide similar military and civilian advantages; the difference lies primarily in how the information is used. Satellites contributes with everything from intelligence, precision navigation and global communication, which both increases and reinforces military capability. Even if a high degree of vulnerability is not acceptable in military contexts, some military capability is critically dependent on satellite services. Many countries are so dependent on satellite-based services that an adversary could use this against them. Without space-based services, many modern armed forces and weapons systems would be forced to adapt themselves and their actions, with impaired effect as a result. Therefore, in a conflict, the use of, or the threat of using, ASAT weapons can force the opponent to alter its actions. By denying satellite-based services to a high-technology actor, the latter's technological advantage can be limited or neutralised. This clarifies the asymmetrical advantages a minor actor obtains by acquiring ASAT capability. Several nations have lately shown that they have the capacity to interfere with or destroy satellites and their services. This pushes the arms race within the space domain further. Internationally, this is used as a motive for developing space defence mechanisms as well as offensive capabilities both on the ground and in space.

Develop a Swedish contingency plan to face the arms race within space

It is difficult to understand how extensively dependent Sweden is on satellite services. It is a challenge to identify and understand complex dependencies for the purpose of minimising the negative consequences for both the civilian and military defence. Awareness of this problem is relatively low and there is no clarity on how this is going to be handled, or by whom, in the planning of the total defence. Sweden needs to take a position on the fact that conflicts are already taking place in space and that crises can arise that are difficult to resolve and that war can start in space. Eventually, such a conflict would affect Sweden.

It would be to our advantage to develop a contingency plan to deal with the actions of other actors in space. A first step in this direction would be that Swedish defence planning and total defence planning take into account a security situation where space represents yet another domain with unique threats.

The contingency plan should contain activities as involving leaders and authorities for increased awareness and knowledge of the impact and significance that the space domain has for future conflicts. This would facilitate strategic decision-making related to the defence and security policy aspects of the space domain. This would also contribute to an understanding of how international space policy developments can eventually affect Sweden and our total defence.

A contingency plan would create coordination and consensus on defence- and security-related space issues within the total defence, regarding not only the practical use of satellite services, but also on research, technology development and the support that is needed to be able to manage the international development within the space domain. This could lead to a better understanding of different responsibilities between involved organisations.

To support defence planning and total defence planning in these issues there is a need for knowledge-building efforts. Examples of areas where such efforts are needed include concepts of warfare in the space domain, the consequences of this and possible measures of defence. Other areas involve theory of space power, different actors' perspectives and the type of action that can lead to increased tension in space. Knowledge about the most critical and exposed systems, in terms of dependencies and vulnerabilities, is also needed. Studies should include risks and threats that Sweden face which are dependent on space in case satellite services are disrupted. National priorities, including the differences between the needs of society and those of the armed forces, must also be determined.

FURTHER READING

Regeringens skrivelse 2017/18:259 En strategi för svensk rymdverksamhet, 2018-05-09, Skr. 2017/18:259, https://www.riksdagen.se/sv/dokument-lagar/dokument/skrivelse/en-strategi-for-svensk-rymdverksamhet_H503259(accessed 2020-05-28).

Faria, D., Hallgren, K. and Lindström, S., 2019, *Förändringar inom rymdområdet och dess påverkan på svensk utrikes- och säkerhetspolitik,* FOI Memo 6993.

Lindström, S. (ed.), 2021, *Omvärldsanalys Rymd 2020 – Fokus på försvar och säkerhet,* FOI-R--5077--SE.

10. Future antagonistic biological and chemical threats

Anders Larsson, Susanne Börjegren and Birgitta Liljedahl

That Sweden might experience an attack with biological or chemical weapons, so-called BC agents, may seem unlikely today. Imagine the following scenario: In 2025, a number of cases of an unusually infectious and difficult to treat variant of multi-resistant TBC is discovered in several of the country's refugee lodgings. Several deaths occur and personnel are also infected. Concern is raised over a general spread of infection in society and there are harder demands for a tightening of asylum immigration. Analyses indicate that the bacteria has similarities to an earlier known variant that ravaged Russian jails in the 1990s, but is suspected to have been manipulated so that the course of the disease is more rapid. The police investigation shows that the disease seems to have been deliberately spread in several asylum residences. But by whom is unknown.

Even if Sweden has so far not been afflicted by any antagonistic attacks with chemical or biological agents, events elsewhere in the world, as well as the rapid pace of technological development that is taking place primarily in the biological field, show that the above scenario cannot be excluded and that it is important to have a readiness to be able to deal with it.

Increased use of chemical agents as weapons

The attempted assassination of the Russian opposition leader Aleksei Navalny in 2020 and of the ex-spy Sergei Skripal and his daughter, in Salisbury in 2018, as well as the murder of the North Korean leader's brother in Malaysia in 2017 are three current examples of the use of nerve agents for the purpose of eliminating unwanted individuals. The Syrian regime's use of sarin and chlorine gas between 2013 and 2019, in addition to the fact that the terror organisation Daesh has produced and used mustard gas in Iraq and Syria, means that the threshold for the use of chemical weapons has been lowered.

The work of the Organisation for the Prohibition of Chemical Weapons, OPCW, to ensure compliance with the chemical weapons convention, is made more difficult by the strong polarisation that has arisen. The variation in materials that are possible to use as chemical weapons is nearly endless, which also restricts the possibilities to envision and create the regulatory structure needed to counter the threats of the future.

Technological leaps in the development of BC agents

Today there already are sufficiently potent chemical and biological weapons and methods for spreading them. The driving force to develop new agents probably does not lie, therefore, in being able to inflict greater damage, but rather to make a future attack more difficult to predict, discover, trace and manage, for example within the frame of the chemical weapons convention.

Biotechnology is the area where development is proceeding most quickly. The CRISPR/Cas9 genetic scissors, which make it possible to edit the DNA of living organisms with great precision, have created the basis for being more or less able to tailor biological organisms and their characteristics. Using synthetic biology, it is possible to both create dangerous new microorganisms and recreate those that have become extinct. Pharmaceutical development leads to new ways to protect against or relieve the effects of bacteria and viruses, for example, but the knowledge gained from research can also be misused to make them more injurious or infectious.

The possibilities for producing new knowledge within biotechnology research have increased during recent years, which is illustrated by the relatively new phenomenon of *Do-it-yourself biology*. This is an informal movement that gathers people from different backgrounds to discuss, experiment and share experience within the fields of biology and biotechnology, outside of traditional research milieu.

The coronavirus pandemic is predicted to lead to greater focus on research and development in the medical field. The global character and complexity of the crisis mean that researchers around the world share information and make data and results public to a greater extent than previously. The hunt for knowledge and antidotes creates the risk that research results may not be reviewed as carefully as under normal circumstances. An important aspect of the review process involves ethics, for example whether the published results can be used for malicious purposes. The pandemic has also demonstrated the enormous consequences that a naturally occurring disease can have for society and the world. A biological weapon, which would probably be deadlier than the virus that is now spreading, would thus have even more serious consequences.

Trends that affect the BC threat

Technology development affects what circumstances are available for taking advantage of, creating and spreading dangerous agents. Digitalisation has meant and also in the future will mean that advanced knowledge within the area of toxic and infectious agents is also publicly available and therefore also possible to misuse.

The rapid development of digital social platforms creates opportunities for sharing information, opinions, disinformation and rumours at a speed that quality-controlled media and authorities' information platforms today lack the ability to keep up with. An important part of the use of BC agents is the psychological effect they have on people, where rumour mongering and disinformation can increase people's fear and worry. A continuing trend with a fast development of informal social information channels is therefore excellent for anyone who wants to use these agents to injure and frighten others.

The future development of antagonistic BC threats is difficult to predict. The quickly increasing use of chemical weapons in military conflicts by both state and non-state actors in Iraq and Syria was a surprise to most. It's not possible to exclude the possibility that in the future certain states would use chemical or biological weapons in a military conflict, even on Swedish territory, if these provides tactical or strategic advantages.

The use of nerve agents in murder and attempts to assassinate political opponents is a worrisome trend and the consequences that society can be affected by were clearly illustrated by the events in Salisbury. Two persons with no connection to the original event were affected four months later in nearby Amesbury, when they accidentally came into contact with the perfume bottle that was used to poison Skripals. One of these persons died. This shows that there are states who do not hesitate to use neurotoxins in peacetime, without caring whether or to what extent innocent civilians are afflicted. That a similar event could happen in Sweden cannot be excluded.

Can Sweden meet the challenge?

In Sweden, we have focussed until now on increasing our ability to handle accidents involving dangerous substances. It is also important that society prepares itself, through education, training and readiness-raising measures, among others, for an intentional, antagonistic use of BC agents. Such an incident can include substances that never occur in accidents. Dealing with such a situation will also be different due to the requirement for meticulous forensic analysis and because of needing to pay attention to the psychological dimension involved.

To develop Sweden's ability to handle events involving chemical, biological and radioactive materials, as well as nuclear weapons and explosive substances, a joint actor CBRNE strategy was formulated in 2017. At that time, the Swedish Civil Contingencies Agency, MSB, joined with other authorities concerned with four objective areas (coordination, threats and risks, capability and control instruments), as well as nine priority areas in which Sweden's capabilities need to be increased. The work was evaluated during 2020, with an emphasis on how well these objectives were attained and how the effort in the priority areas had proceeded. The evaluation is intended to result in a recommendation of what needs to be altered in the strategy. Much remains to be done, but the progress made in recent years, for example on certain coordination between national and regional levels, constitutes an important pillar in the continuing capacity-raising effort. In the management of the coronavirus pandemic, several examples of where the importance of cooperation and pre-determined division of roles and responsibilities have become clear. Something that also remains to deal with is the appearance of objectives and guidelines for what civil society is expected to be able to handle, which presupposes clear directives from decision-makers on political level.

The coronavirus pandemic has exposed society's vulnerability during the event of a serious spread of infection and in a tangible way highlighted the consequences of, for example, heavily reduced contingency stores. The coronavirus pandemic, the continuing work in total defence planning, and the fact that chemical weapons have recently been used several times have led to an increased awareness among many actors. This awareness also needs to be translated into work that in a structured way increases civil society's ability to handle incidents involving biological and chemical weapons.

New drastic changes in the use of hazardous materials by antagonists must also be followed up and future changes in approach must be predicted as far as possible. This area needs to be continuously followed up and analysed from a total defence perspective. Capacity-raising measures need to be prioritised, based on assessment of the future threat. It is not enough to prepare oneself for what has already happened.

FURTHER READING

Normark, M., Lindblad, A., Sandström, B., Tunemalm, A.K., Wiktelius, D., Wikström, P. and Vesterlund, A., 2020, *CBRN-hot från ickestatliga aktörer – Årsrapport 2019*, FOI-R--4953--SE.

Börjegren, S., Holmgren Rondahl, S., Larsson, A., Liljedahl, B., Normark, M., Tunemalm, A.K., Sandström, B., Waleij, A. and Wikström, P., 2019, *Totalförsvarsplanering med fokus på CBRN – Framtida antagonistiska CBRN-hot*, FOI-R--4765--SE.

Waleij, A., Liljedahl, B., Börjegren, S. and Lindahl, D., 2019, *Vidare kontext för en CBRN-relaterad hotbild*, FOI-R--4781--SE.

11. A threat cascade against global health in the era of disinformation

Annica Waleij

One of the top global health threats identified by the World Health Organization (WHO) are infectious diseases. At both global and national levels, 2020 was dominated by the coronavirus pandemic, which by the beginning of December had infected more than 63 million people worldwide and claimed more than 1.4 million lives. In the wake of the pandemic, the global economy has been hard hit, and enormous amounts of disinformation have flourished. The pandemic, however, has not meant that other health threats have vanished. That global health threats are not one specific threat, but a tapestry of interwoven threats that often reinforce each other, has perhaps never been more evident. This means that the basic causes of illness must be understood in a greater context than what is comprised of its individual contributing components, and also that the solutions to poor health are multiple and must interact in both time and space.

Health is said to be one of those things one does not really reflect on, until it is gone. On the other hand, one thinks of it more than ever when it is gone. According to the WHO, health "is a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity". In other words, it is not enough to be free from illness; one should also feel good. Measuring people's health is difficult, since it usually involves individual experiences. Global health is therefore measured in various ways and includes many different aspects of societal development across the world.

Health is politics!

Health is a fundamental human right, which means that health aspects easily become politicised. Health is not a product or a service that is available to the same extent for everyone, everywhere. Certain individuals and groups are generally in better health than others. So-called socially determinants of health, that is, the prevailing circumstances such as where a person is born, grows up, lives, works, worships and ages are different not only between countries but also within them.

Internationally, health diplomacy is a tool used for political aims as a form of soft power, to promote public health and strengthen weak health systems, or to pour oil on troubled waters when diplomatic relations between countries become frosty. Health can also be used to leverage other political issues or as a means to apply political pressure.

Ultimately, limiting access to health is a concrete and effective weapon. In civil-war plagued Syria, the Assad regime is trying to control parts of the population by denying them access to health care. Medical personnel and health care facilities are often direct targets for acts of war. A trend in war zones in general is that the protection and laws of the Geneva Convention are increasingly ignored. Atrocities are committed by different sides in conflicts, with no apparent consequences for the perpetrators, that is, with impunity. For example, in the spring of 2020, a politically motivated attack was carried out against a maternity clinic in Kabul, Afghanistan.

The connection between national security and disease surveillance on the one hand and bioterrorism on the other became obvious with the circulation of the so-called anthrax letters in the US and also in Sweden in the early 2000s. The events in the US also became politicised, through conspiracy theories about genetically manipulated anthrax spores and insinuations of the involvement of a foreign power. In Sweden, health threats have their own section in the Swedish national security strategy, which seems natural given that one of the objectives of Sweden's societal security is to protect the lives and health of the population. It states, among other things, that health threats have a transboundary dimension and that the nature of the threats is to a great extent unpredictable, since microorganisms continuously change.

The coronavirus pandemic has displayed many examples of politicisation. Just a few examples include then President Trump's decision to cease financing and, later, to completely leave the WHO, and China's countermove to offer compensation for the economic shortfall. The dismantling of democratic processes, where authoritarian states refer to the coronavirus to justify pushing through dubious emergency laws or to install different types of surveillance systems to monitor its citizens are some further examples. Even if the measures have contributed to fighting the spread of infection, there remains an antidemocratic flipside, such as for example certain heads of state who have taken advantage of the situation to increase their power.

A tapestry of interwoven threats

WHO has listed ten of the most imminent threats to global health. It includes, in addition to infectious diseases such as the ebola haemorrhagic fever, dengue fever, AIDS and influenza, other types of health threats, such as weak healthcare systems, fragile and conflict-stricken states, increased antibiotic resistance, air pollution and climate change, as well as non-communicable diseases, welfare diseases and vaccination resistance. Several other associated threats and risks have been identified by the World Economic Forum (WEF), and include accelerated biological diversity loss of biodiversity, the increasing gap between rich and poor, mental illness, extreme weather events, cyber threats, as well as CBRN threats, that is, events involving infectious biological, toxic chemicals, or radioactive substances.

The global health threat, despite its name, is not one specific threat, but an entire tapestry of interwoven threats. In some cases, the threats reinforce one another, but there can also be opposing forces. The need for a holistic approach to global health threats has thus been identified in various global initiatives, for example the UN's agenda for sustainable development, Agenda 2030, consisting of 17 measurable goals. Another example is the *One Health Approach*, which recognizes that the health of people is closely interconnected to the health of animals in our shared environment, where a change in one ecosystem affects the other system.

In the wake of the coronavirus pandemic it has become obvious how vulnerable our societies are, and also how closely linked many health threats are. Weak health systems leave countries less-equipped to withstand challenges such as those that arise when different threats coincide, for example extreme weather events and threats to health. Many normally associate such vulnerabilities with developing countries and conflict regions. The coronavirus pandemic, however, has shown that there also are extensive vulnerabilities in more developed countries. Effects on public health has been observed when important vaccination programmes against other diseases have not been carried out as planned, or when people, out of fear, refrain from seeking vital health care for other conditions, which results in increased poverty and in the occurrences of diseases that are otherwise preventable. It is not only the coronavirus itself, but also the responses to it, which have consequences for society. Closed borders, countries in lockdown and stranded migrants increase the risk of unharvested crops, food insecurity and immense human suffering.

An aging population and welfare diseases are other problems, also in developing countries. It is a paradox that, at the same time as large portions of a population may be suffering from malnutrition, obesity is increasing, and that both problems can sometimes be observed in the one and same person. Medicines play an important part both in fighting acute and chronic diseases and in relieving the effects of natural aging. However, global pharmaceutical production is vulnerable, since the production of critical pharmaceutical raw materials is mainly concentrated to a small number of companies. Dependence on China for certain ingredients and on India for manufacturing of medicines is for example strong. Another vulnerability is the clear link to the natural environment and the escalating depletion of biological diversity. Almost 50 percent of original key substances in today's medicines have natural sources, and future innovation will continue to rely on lessons from nature for inspiration. Preserving the natural environment and the ecosystem services nature provides is central for both pharmaceutical innovation and food production. Reduced numbers of pollinating bees adds to the risk of increased food insecurity, which in turn can lead to increased malnutrition and mortality and is especially serious in fragile regions with weak health care systems. Local uprisings are not uncommon in the wake of acute food and water shortages.

Who can one trust?

The development of vaccines is one of humanity's greatest health-promoting scientific breakthroughs. Smallpox has been eradicated and polio, which was a very common disease in the beginning of the 1900s, now occurs naturally in just two countries. Measles, which is extremely infectious, has in principle been controlled, thanks to worldwide vaccination coverage. A vaccine against ebola exists.

At the same time, there are examples of setbacks: for example, several well-developed countries can no longer claim to be free from measles. Polio has regained a foothold in conflict-ridden areas such as eastern Ukraine, and the latest ebola outbreak in the Democratic Republic of the Congo (DRC) had its worst impact in those areas that were impacted by conflict. These trends are fuelled by a growing anti-vaccination movements, not rarely driven by a combination of ignorance and disinformation. That people refrain from vaccinating themselves and their children may be due to a lack of confidence in the safety of the vaccines or to religious motives. People can refuse to be vaccinated or to take prescribed medicines, but at the same time test ineffective or directly dangerous substances in hope of obtaining results. This affects not only the individual, but also contributes to impairing herd immunity, which affects the whole society. Polarisation between those who are for and those who are against vaccines is increasing and risks creating schisms in society.

In the wake of the coronavirus pandemic, both misinformation and disinformation campaigns have flourished. The WHO classified the coronavirus pandemic early on as an infodemic, that is, a pandemic of disinformation, with internet as the playing field. A portal on WHO's homepage has been created to counter the most commonly occurring myths. The Public Health Agency of Sweden, the Swedish Civil Contingencies Agency and EU have also taken initiatives to counter false information. A generally accepted theory is that the the coronavirus originated in a fish market in Wuhan, where wild animals also were sold. There are also more conspiratorial narratives, ranging from those saying that the virus was spread by an American participant in the military World Games, held in Wuhan in the fall of 2019, to theories that the virus escaped from a high-security laboratory or that it was produced as a biological weapon.

Conspiracy theories about diseases and pandemics are nothing new. The most common conspiracy theory around HIV is for example that the virus was created through biological weapons experiments in the USA and that the infection was then spread by the Central Intelligence Agency, the CIA. The theory, which in fact was a product by the Soviet intelligence agency, the KGB, spread globally in the mid 1980s.

Less well-known events include the false information that strongly contributed to the exacerbation of the measles outbreak in the island nation Samoa at the end of 2019. Vaccination coverage was low in Samoa to begin with and the measles outbreak was further worsened by disinformation. Social media, including the government's Facebook page, was flooded with anti-vaccination propaganda from accounts that appeared to be registered in the USA. Another example is the latest ebola outbreak in the DRC, where rumours were circulating that the ebola vaccine causes sterility and that the virus was produced by the Congolese government. These two erroneous claims hindered the effort against the virus in the DRC, and also led to violence against healthcare personnel.

Conspiration theories have consequences by undermining serious research and making it difficult to reach out with correct information. There are many examples where health and medical personnel have been stigmatised, exposed to cyber hate, threats and physical, even deadly, violence.

Soap, a pretty neat innovation!

As a result of the coronavirus pandemic, a temporary decline in the development curves related to Agenda 2030 and the Millennium Development Goals expected. In the short term, it may get worse before it gets better. Healthcare systems are going to experience long-lasting consequences regarding personnel and financial resources. The magnitude of effects on mental health are difficult to foresee, but considerable domino effects on public health can be anticipated.

Well, then, does this mean we're in a terrible mess? Or maybe the other way around? A glance into the visual statistic tool *Gapminder*, which Hans Rosling, the Swedish optimist, doctor and professor in international health, helped to found, shows among other things that average life expectancy in the world is increasing and that infant mortality – an indicator of welfare – is decreasing. More girls are going to school and increasing numbers of people are being lifted out of absolute poverty, more people are getting better living conditions and more people have a belief in the future.

There are other examples of technological leaps and advanced technology developments of significance for reducing the consequences of the health threats listed by the WHO. A few examples include genetic engineering, artificial intelligence (AI) and artificial pollination of plants, using mechanical bees. Technological development can even in many cases contribute to reducing health threats themselves.

At times, it can be easy to forget that it is not always the latest and most advanced inventions that provide the best solutions. The first known recipe for producing soap is assumed to originate from Babylonia, around 2200 BC. As the coronavirus pandemic has shown, soap and water, properly used, are one of the most important interventions for limiting the spread of the virus. Maintaining basic personal hygiene and keeping distance prevent also other infectious diseases, such as winter vomiting disease (Norwalk virus), diarrhoeal diseases, and seasonal influenza.

Despite all the negative effects the coronavirus has brought with it, however, there are also positive changes, such as changed lifestyle patterns. Some of these will probably last over time: more distance work and changed travel habits are examples that need not be negative.

Health threats are influenced by globalisation and what is needed is a holistic overall approach that is based on a broad perspective on the threats, solutions and capabilities. In addition, every country must also break down the threats to national level. According to Sweden's national security strategy, a national capacity to prevent, identify and mitigate health threats is required as well as a robust preparedness for action against health threats. Furthermore, well-functioning interdisciplinary cooperation at national, European and global levels is needed. This is where Sweden, as a pioneer in many international health-promoting initiatives, has a role to play.

FURTHER READING

Wikström, P., 2020, *Kommer coronaviruset från ett laboratorium eller ej?*
FOI Memo 7239.

Rosling, H., Rosling, O. and Rosling Rönnlund, A., 2019, *Factfulness: Ten Reasons We're Wrong About The World - And Why Things Are Better Than You Think.* Hodder & Stoughton. ISBN: 9781473637474

Bucht, G., Waleij, A. and Frithz, E., 2016, *Ebola - Science, society and security*.
FOI MEMO 5911

12. Supersoldiers

Britta Levin, Sofia Hedenstierna, Ove Jansson and Martin Hagström

Humans have long sought to increase their physical and cognitive abilities with the help of technical aids, physical bodily interventions or mental training. Technological development is about to change the range of possible human augmentations and hence the subsequent types of enhanced abilities. The armies of the future may very well consist of supersoldiers from science fiction.

Supersoldiers have the potential to change the military power balance between actors who augment and those who do not. What different enhancements mean in terms of military applications and potential ethical dilemmas needs to be studied thoroughly. Which actors will be inclined to augment their soldiers to supersoldiers and what will the implications be if refraining from doing so?

Human performance enhancement – a hot area of development

The principle of human enhancement is not new – large-scale experiments with pharmaceutical substances and mechanical reinforcement have been conducted during times of armed conflict. In many cases, individuals have themselves chosen to use drugs, but there has also been examples of organised use. During the Second World War, for example, methamphetamine was used to provide extra energy, wide-awakeness, focus and courage. However, side-effects in the form of hubris, aggressiveness and exhaustion occurred on a large scale, accompanied by a lack of judgement that led soldiers to engage in combat that were impossible to win. Contemporary attempts to enhance soldiers' abilities mainly focus on other methods and techniques.

The interdisciplinary developments in medicine and technology have led to new possibilities for treating diseases and replacing injured parts of the body. Some of these technologies and methods can also be used to increase the performance of healthy individuals to biologically above-normal levels. Development within this field has generated great interest but is largely taking place in the civil sector. Countries such as the USA, China and Russia are investing heavily in research on future technologies for military applications. Examples of technology areas where the pace of development is high and critical for human enhancement include biotechnology, miniaturisation of electronics, artificial intelligence, materials technology and power supply.

Enhancement today and tomorrow

Research is paving the way for progress in both already existing technologies and in new areas that are still in their infancy, but that have the potential to fundamentally change human functions or biology. Enhancement is expected to increase soldiers' ability to perform their tasks by giving them tools for dealing with physical as well as mental strain. The field is broad and involves anything from increased attention to longer endurance, as well as abilities that cannot even be imagined today.

Exoskeleton, a term borrowed from biology, denotes a structure placed on the outside of the body. An exoskeleton can be used to give a person postural stability, provide physical protection and generate superhuman strength. Today, there exist exoskeletons for military personnel, in the form of supporting frames and springs, that carry the weight of heavy equipment and thus prevent stress injuries. Development of the next generation of soldier systems include powered exoskeletons, where built-in motors can generate forces that amplify, for example, lifting or jumping ability. Today's powered exoskeletons are bulky and heavily energy-consuming, but the trend is towards more agile and less energy-reliant systems. Assisted by artificial intelligence, an exoskeleton can be trained to act together with an individual so that they move as an integrated unit, with superhuman strength and agility.

Bionic body parts are implants or robotic components that are linked to the nervous system with neural implants and thus can be controlled by the human will. Currently, they exist in simpler forms that replace lost body parts and include mind-controlled artificial arms, with hands that can grasp and move objects. As technology advances, bionic body parts will be improved with increased neural control and greater mobility and strength. One possible future development is a combination of an exoskeleton and a neural implant, so that the exoskeleton is controlled by the brain and leads to both superhuman strength and speed.

Neural implants that replace bodily senses already exist, in the form of for example cochlear implants that send signals directly from microphones to the auditory nerve. Systems with camera-equipped glasses that send signals to the optic nerve are being developed. Neural implants can also be used with sensors that expand the human range of perception with for example vision in the infrared spectrum or the ability to perceive ultrasound. A new type of biocompatible lens, surgically implanted in the eye, is nearing clinical trials. The lens is said to be the first step towards improved sight and the ability to project information and interact with the surroundings. These developments likely still lie a bit further into the future and depend on continued electronic and sensor miniaturisation as well as improved solutions for power supply.

Progress in genetic engineering is expected to revolutionise the opportunities for changing and tailoring the characteristics of organisms, and this in the near future. Genes can be modified or replaced with custom-made genes that have been constructed to produce a desired improvement. The new gene-editing method, the so-called genetic scissors, CRISPR/Cas9, has been shown to be effective in creating targeted modifications in genetic material. Myostatin is a protein that regulates the growth of muscle mass. In a test involving a dog, a beagle, at the Guangzhou Institute of Biomedicine and Health, the gene that produces myostatin was turned off, which caused the dog's muscles to double in size.

Applications for human augmentation are found in both an active research world and within a do-it-yourself culture that includes various approaches to augmenting oneself in order to become healthier, stronger and smarter. This field includes everything from taking vitamins to illegal substances and experiments in genetic modification. The training culture is far ahead in its pursuit of optimal performance and uses, among other things, advanced smartphone applications to create recommended training routines customised to the individual's performance curve.

Military applications – a threat

Future technologies open up opportunities to create people who are physically and cognitively superior to those living today. In military applications, the power balance can change dramatically if states or non-state groupings choose to create supersoldiers on the basis of the new technologies. Many human performance enhancement technologies are and will continue to be costly and reserved to economically strong actors and a limited number of soldiers, while other technologies that are in use today as self-medication may be relatively inexpensive but unsafe, both in terms of effect and quality and, thus, more risky. An actor who wants to increase the performance of its military forces through human performance enhancement can utilise these technology developments in various ways, either by raising the basic level of soldiers in the regular forces or through the specialisation of only a few chosen individuals for a unique task.

Concretely, a supersoldier would be able to move themselves further and longer as well as act with greater strength, stamina and decisiveness compared to a normal person. Soldiers with superhuman muscle strength, for example with the help of an exoskeleton, can carry heavier protective equipment and weapons, which results in both increased efficacy and lower vulnerability. Apart from greater physical capabilities, a supersoldier could possess sharper or increased faculties, for example by being able to see infrared light or hear ultrasound, as well as higher cognitive ability to manage large amounts of information and make decisions even under hard mental pressure.

Modern war illustrates how armed conflict often takes place in urban terrain. Large mechanical fighting platforms, such as tanks, are cumbersome to manoeuvre in built-up environments. A supersoldier, on the other hand, moves easily in the city environment, is agile enough to be effective at close quarter battle, while strong enough to bear weapons that deliver larger effect even at greater distances. That way, a supersoldier's efficacy can be said to be the equivalent of several conventional soldiers or a vehicle, but moves more easily without being detected. Furthermore, highly specialised soldiers with enhanced senses and improved cognitive ability have better qualities for conducting advanced operations, for example against selected high-priority targets.

The psychological aspect of supersoldiers is important. The threat of meeting a both mentally and physically superior soldier on the battlefield risks affecting fighting morale negatively. If the power balance at the individual level is greatly uneven, to the enemy's advantage, or if an enemy is considered to be inhuman, the view of whether the battle can be won is affected. This can in turn influence the psychological resilience among the fighting units as well as in the civilian society.

How to meet the threat

Human performance enhancement already occurs privately in Sweden and it is not unthinkable that the Swedish Armed Forces may introduce a number of less controversial techniques on a broad scale. However, similarly to other military technology development there is always a substantial risk that a future opponent will have gone further and gained advantage through more extreme enhancement at the expense of the individual.

A threat in the form of supersoldiers must not necessarily be met by creating one's own supersoldiers. Training and traditional methods for attaining soldiers' highest possible capabilities, in combination with state-of-the-art technologies, such as fire control systems that detect and assist in hitting the target and unmanned systems that replace the soldier on the front line, can create advantages that compensate for the enemy's abilities. However, confronting an enemy who has supersoldiers who are superior both in terms of lethality and protection capabilities requires the development of combat techniques, with new combinations of weapon systems and methods for using them. If the combat range is increased to the point that our weapons do not achieve any effect, we are required to manoeuvre our forces closer to the threat, or engage with larger units equipped with more advanced platforms.

Ethical principles and options

The development of technologies that enhance the human body entails several ethical dilemmas. Just as the technology can be positive and decisive in curing disease and improving the quality of life for great numbers of people, it can also be negative and dangerous if it is used in an uncontrolled or destructive manner. Changes to the body can pose risks to the individual, in the form of side effects, injuries caused by malfunctions, or modifications that are so extreme that they have a negative impact on the general quality of life. The use of gene technology is not uncontroversial at either the level of the individual or of society as a whole: it is one thing to change a single individual and another to modify the genetic make-up of the entire organism, so that the change remains across future generations.

In the case of supersoldiers, the risk for the individual is weighed against the presumed benefits and utility for defending the country's sovereignty. Certain risks may be acceptable if the eventual benefits are large enough, but the question is to what extent an enhancement of military capability can justify a risk for the individual. Another question regards what applies when the soldier no longer remains in active service; who is then responsible for a possibly life-long need for medication and upgrades, or readjustment to society?

Medical risks and ethical considerations influence the possibilities to implement the new technologies. The knowledge in this area must be developed in order to be able to evaluate the opportunities provided by the technologies and design principles for research. Several different sets of principles become relevant when human augmentation in military applications is involved, everything from the efforts based on the UN's Universal Declaration of Human Rights (1948), and the Nuremberg Code (1947) on human experimentation, to the World Medical Association International Code of Medical Ethics (1948). The transposition of international agreements into national legislation, however, varies between countries.

Sweden has strict restrictions on the conduct of research and development in technologies that can affect humans and their integrity. An enemy with other values and regulations would be able to achieve a developmental advantage by conducting riskier experiments and implementation of technology that in our eyes is unethical. Similar problems arise regarding other technologies, for example in the use of autonomous systems in military applications.

Fiction becomes reality

The technology of human performance enhancement is under development and is approaching what is currently considered fiction. It is too early to know how the technology is going to be used by various actors in military applications, but the possibility that it will constitute a military threat cannot be excluded. It is therefore high time to initiate a discussion on how the technology, in the form of choice of arena, materiel and methods may influence combat in future. Part of this effort is to evaluate the value of potential augmentations and methods. Technological expertise is required to be able to assess both threats and potential uses. It is thus important to continue to develop this area through controlled and transparent research.

Human performance enhancement in the military domain means that the terms and conditions are going to change. Functional control mechanisms are needed to utilise the new technology in the best way. Today, various international regulations on research in medical applications exist, but clear international agreements on military applications are missing and must be created in the context of international law. In order to conduct research and development without generating tensions in security policy, an international discussion on the direction of research is needed. In the end, different states need to assess which path they are going to choose to confront the threat: either through their own supersoldiers, choosing other materiel and combat technologies, or a combination of both.

Further reading

Levin, B., Hedenstierna, S., Hagström, M., Svensson, J. and Hermelin, J., 2018, *Förstärkning av mänsklig förmåga – en framtidsvy,* FOI-R--4716--SE.

Matthews, M. D. and Schnyer, D. M. (eds.), 2018, *Human Performance Optimization: The Science and Ethics of Enhancing Human Capabilities*. Oxford University Press.

Mehlman, M., Lin, P. and Abney, K., 2013, *Enhanced warfighters: Risk, ethics, and policy.* Case Legal Studies Research Paper, 2013–2.

13. Future Threats and Some Considerations for the Next U.S. National Defense Strategy

Gene Germanovich, Gabrielle Tarini and K. Jack Riley

Even prior to the COVID-19 pandemic, the security and defense environment the United States faced was characterized by a range of sophisticated, evolving state and non-state threats and transnational challenges. The U.S. Department of Defense's 2018 National Defense Strategy (NDS) articulates goals for U.S. military planning, and identifies capabilities required to support the approach set forth in the broader National Security Strategy. The RAND Corporation, a non-profit, non-partisan research organization, supported the framing, shaping, and implementation of the NDS, which represented a noteworthy shift in focus for the Pentagon. In this article we offer a U.S. perspective on the evolution of threats from the recent past, and posit several considerations for the next NDS, expected sometime within the next year.

Evolution of U.S. Threat Perceptions

In the wake of the September 11, 2001 attacks, U.S. national security policy reoriented toward a global counterterrorism campaign and counterinsurgency operations in Southwest Asia and the Middle East. The United States sought a global coalition against terrorism, which included China and Russia, and most elements of strategic competition were deemphasized. As early as 2011, uncertain about a rising China's intentions and recognizing that U.S. economic and security interests were increasingly linked to the Asia-Pacific, the United States endeavored to adopt a more balanced security posture. Then-Secretary of State Hillary Clinton summarized the logic of the nation's so-called rebalance to the Pacific: "The future of politics will be decided in Asia, not Afghanistan or Iraq, and the United States will be right at the center of the action." The Pentagon codified this rebalance in its 2012 Defense Strategic Guidance. This shift reflected a growing skepticism toward previously held U.S. and Western assumptions about how China's integration into the global economy would result in a benign presence on the global stage and harmonious Sino-American relations.

But despite U.S. intentions to shift its strategic focus to Asia, the Arab Spring, military intervention in Libya, failure to stabilize Afghanistan, and rise of ISIS made it difficult to follow through. Russia's aggression in Ukraine, hostile actions against NATO and Europe, and military modernization – not to mention the development of North Korean and Iranian nuclear and missile programs – continued to test Washington's strategic calculus and stretch its resources. Technological advancements and adversarial pursuit and, in some cases, aggressive use of space and cyberspace capabilities also contributed to the growing list of security concerns.

The 2018 NDS represented an unambiguous prioritization of this array of threats. The United States intends to orient its military on China, Russia, and then everything else, in that order. The strategy, promulgated by Secretary of Defense Jim Mattis, emphasized: "Long term strategic competitions with China and Russia are the principal priorities for the Department and require both increased and sustained investment, because of the magnitude of the threats they pose to U.S. security and prosperity today, and the potential for those threats to increase in the future." Current Secretary of Defense Mark Esper has clarified which of the two competing powers would be the foremost driver of U.S. defense choices by repeatedly denoting the Indo-Pacific region as America's "priority theater."

Recent Orientation and Current Outlook

Competition with China will be ongoing and open-ended, and likely represents a generation or longer endeavor. The Department of Defense has indeed stepped up its focus on the Indo-Pacific, and dedicated new resources—money, forces, and senior leader attention—to engage in the evolving strategic competition with China. The military is adopting a deterrent posture with augmented deployments and preparations for a future conflict in Asia. Ongoing changes within the U.S. Marine Corps represent one prominent example of the importance of the Pacific in U.S. defense strategy. After two decades of land warfare in Afghanistan and Iraq, the Commandant of the U.S. Marine Corps initiated an overhaul of the 186,000-strong branch of the armed forces. As part of his strategy, the Marines' force design, procurement, training, and posture will be tailored to competing and, if needed, warfighting with China.

Yet no strategy can have an entirely singular focus. Other actors called out in the 2018 NDS—Russia, North Korea, Iran, and global terrorist organizations—threaten the United States and its allies. Although it is difficult to anticipate the future security environment, most American experts broadly agree that each of these actors will continue to pursue objectives that are incompatible with U.S. interests. None of these threats will materially diminish in the coming decade, but given the strategic emphasis on China, U.S. policymakers are increasingly willing to accept greater risk and economize efforts in these areas. The strategy also highlights the threat of weapons of mass destruction proliferation and hybrid challenges such as disinformation campaigns and economic coercion. Such "irregular warfare" tactics require the U.S. military to maintain capabilities relevant for strategically competing below the threshold of armed conflict. These will remain issues of concern, albeit with the understanding that the Department of Defense will generally play a supporting role to other agencies.

Some common threads tie together each of the threat actors identified by the NDS. State adversaries and sophisticated non-state actors increasingly possess capabilities that make U.S. power projection less tenable. Long-range precision strike weapons deployed on increasing numbers of smaller, mobile platforms and enabled by persistent surveillance and targeting networks challenge key tenants of U.S. military advantage. Such capabilities will make it increasingly difficult if not prohibitive for U.S. forces to enter theaters of operations during a crisis. China and Russia's extensive investments in these systems have the potential to create large "no go" zones for U.S. and friendly conventional ground, air, and naval forces. Even smaller states and non-state actors can acquire and employ these weapons for significant effect, as several Houthi rebel missile attacks on U.S. and Saudi warships in the Gulf of Yemen have vividly demonstrated. While the U.S. defense establishment has begun to tackle these dilemmas, maintaining interoperability with NATO and other key allies remains a prime challenge in need of constant attention through joint development of technologies, operational concepts, and training plans.

Looking ahead, COVID-19 will have a significant near- and far-term impacts on U.S. defense strategy. In addition to negatively affecting U.S. military readiness, the current pandemic and future waves of the disease will place renewed demands on the military to support civilian authorities for disaster response, an issue not emphasized in the current NDS. More broadly, the pandemic could accelerate worrisome global trends such as populism, the deterioration of U.S.-China relations, the slowing of European integration and defense cooperation, and the incidence of weak or failing states–all of which contribute to a more dangerous and complex threat landscape for United States, NATO, and other allies and partners. Further, a prolonged crisis could ignite calls for governments to focus inwards, despite the fact that now more than ever, domestic well-being is affected by the rest of the world. COVID-19 and its geopolitical fallout cannot be solved with military tools alone, but the Department of Defense has and will need to continue to play an important supporting role. Tasks may include contingency planning, global transportation, medical assistance, construction, and, potentially, stabilization missions abroad.

From an economic and budgetary perspective, the pandemic will likely intensify existing domestic pressure to overhaul the U.S. healthcare system, expand the social safety net, and prepare for future pandemics. Continuing to spend half of the nation's discretionary budget on defense may become politically and financially unsustainable. Even if Americans continue to support current levels of defense spending, the U.S. government may be unable to afford it due to a ballooning national debt. This fiscal reality poses significant risks for executing the NDS. American decisionmakers will need to make hard choices about which of the strategy's priorities will need to be reexamined. Additionally, the defense policy establishment, including the research community, will need to focus on designing innovative concepts and identifying creative methods that address multiple threats as efficiently as possible.

Considerations for the Next NDS

The architects of national security policy and authors of the next NDS will face a herculean task, potentially while still in the midst of a pandemic and likely a prolonged economic recession. The next National Security Strategy and initial NDS deliberations will need to focus on setting a level of ambition within the projected available resources. One plausible outcome of these reviews might be that some of the goals outlined in the 2018 NDS need to be scaled back. Additionally, some defense funding could be repurposed to support civilian agencies with national and international health security tasks, as well as to account for COVID-related challenges internal to the military.

Three considerations, or guiding principles, may help. While these suggestions do not substitute for fundamental decisions about the extent to which U.S. objectives vis-a-vis the range of military and non-military threats outlined above will need to change, they will help make the most of the resources available for achieving the nation's defense goals as informed by the forthcoming National Security Strategy.

First, the next NDS should strive for concepts, systems, and organizations capable of addressing a spectrum of conflicts and adversaries. China's economic and military clout make it the most dangerous threat facing the United States, but a war with China is not necessarily the most likely scenario to materialize. Rather than attempting to optimize every weapons system, posture decision, and training regimen for a potential China conflict, the U.S. could take a more flexible approach to address a broader range of threat actors while still prioritizing the Pacific. Developing operational concepts that apply to multiple theaters, tailored by region and to specific threat actors, will be a more sustainable long-term approach that leaves fiscal and intellectual space to address pressing needs in other parts of the world. For example, the U.S. Army's development of its Multi Domain Operations concept involves standing up experimental Task Forces in both the Pacific and Europe. Each Task Force will be tailored to deter China and Russia, respectively, but both aim to undermine similar technologies and adversarial concepts intended to deny U.S. forces operational access during a crisis.

Second, affordability will be a greater concern than in the recent past, and not just for the United States, but for its allies as well. In the United States, defense expenditures will be judged against their contributions to difficult-to-measure concepts such as lethality, readiness, and, increasingly, resilience. Allies' ability to support and enable these concepts will depend to considerable extent on their own budget situations and interpretation of regional and other threats. Harmonizing allied support for the NDS will continue to require considerable attention through bilateral consultations and, in the case of NATO, collective defense planning processes.

Third, the strategy will need to emphasize international cooperation. Washington and its allies do not always see threats from shared adversaries in the same way. But faced with a rising China and dangerous Russia—each of whom have few allies of their own—the United States will need to reinforce and recommit to its partnerships. Fulfilling U.S. strategic ambitions in the Pacific will require dedicated maintenance and cultivation of a network of bilateral security partnerships and multinational groupings. NATO remains the lynchpin for deterring Russia, and many allies increasingly view China as a threat, not just a challenge, to European and transatlantic prosperity and security. Finally, international cooperation will need to go beyond traditional military threats. The pandemic underscores global interdependencies and demonstrates the perils of a stunted international response to borderless threats like disease outbreaks and climate change. The next NDS should acknowledge hard geopolitical realities while reinforcing the central role for global institutions and coalitions rooted in shared values and interests in coping with a wide range of challenges where the military will likely be engaged.

The trifocal lens suggested here – flexibility, affordability, and international cooperation – offers a framework the NDS could incorporate to assist in addressing the range of traditional and new security challenges. At the level of research institutions, collaboration across the Atlantic and beyond can serve as a useful mechanism to generate the kind of independent, evidence-based insights that the United States and its defense partners will require to advance common objectives in a flexible, affordable, and cooperative manner.

Further reading

Cohen, R. S., Chandler, N., Efron, S., Frederick, B., Han, E., Klein, K., Morgan, F. E., Rhoades, A. L., Shatz, H. J. and Shokh, Y., 2020, *The Future of Warfare in 2030 Project Overview and Conclusions, RAND Corporation,* DOI: https://doi.org/10.7249/RR2849.

Dobbins, J., Tarini, G. and Wyne, A., 2020, *The Lost Generation in American Foreign Policy How American Influence Has Declined, and What Can Be Done About It,* RAND Corporation, DOI: https://doi.org/10.7249/PEA232-1.

RAND Corporation, 2020, *Supporting the National Defense Strategy,* DOI: https://doi.org/CPA174-1.

Contributors

Matts Björck has a doctorate in technology (physics) from Uppsala University and is a scientist in FOI's Department of Electrooptical Systems. His current research deals with laser weapons, especially action and power-scaling with the help of coherent beam combination. He earlier conducted research within thin film physics and worked with research and development of friction stir welding, at SKB AB.

Susanne Börjegren is a chemist and scientist in FOI's Department of Chemical Threats and Effect Assessments. She works in several areas connected to chemical weapons. Among other things, she provides technical support to the Foreign Ministry in the work with disarmament of chemical weapons within the framework of the OPCW, and is also engaged in several other ways in issues dealing with how protection against chemical weapons should be integrated in planning total defence.

Lars Forssell is a scientist in FOI's Department of Systems Technology. He has a degree in aerospace engineering from KTH Royal Institute of Technology. He has led both national and international research projects in aerospace engineering and automation as well as worked with valuation and analysis of the Swedish Armed Forces weapons and protection systems.

Gene Germanovich is an international defense researcher at the RAND Corporation. His research areas of interest include European security, the NATO alliance, maritime and amphibious forces, and security cooperation. Prior to joining RAND, he spent eleven years at a national security consulting firm where he conducted policy analysis, strategic planning, and wargaming for the Office of the Secretary of Defense, Marine Corps, and other U.S. government clients. He earned a B.S. in international affairs from Georgia Tech and an M.A. in security studies from Georgetown University.

David Gustafsson is a senior scientist and project leader in FOI's Department of Sensor Informatics. He works mainly with machine learning methods, such as deep learning, to analyse images of different modality. He has a master's degree in computer science from Lund University and a doctorate in computer science (emphasis on image analysis) from the University of Copenhagen.

Martin Hagström is a deputy research director in FOI's Department of Systems Technology. He is responsible for the research programme in weapons and protection, as well as unmanned autonomous aircraft, with a background in systems theory. In recent years, his work has included, among other things, ethical and legal aspects of weapons automation and the role of human responsibility in control systems. Martin has a degree in aerospace engineering and mathematical systems theory from KTH Royal Institute of Technology.

Kristofer Hallgren is a senior scientist in FOI's Department of Aerospace Engineering. He has a doctorate from the Max Planck Institute for Solar System Research, in Göttingen, and a civil engineering degree from Luleå University of Technology. Kristofer's focus area is global trends analysis with an emphasis on space as well as space situational awareness. Among other things, he has been responsible for development projects within space situational awareness and supported the the Armed Forces in its strategic work on space questions.

Sofia Hedenstierna is a deputy research director in FOI's Department of Performance Analysis and Systems Assessment. She has a doctorate in biomechanics from KTH Royal Institute of Technology. Her areas of expertise include human vulnerability, action and vulnerability valuation, and body armour and portable weapons systems. She has worked in integrated project teams (IPT) with the Armed Forces and the Swedish Defence Materiel Administration (FMV) regarding objectives for soldier equipment. Se has also worked internationally, for example in EU and international projects.

Vidar Hedtjärn Swaling is a deputy research director in FOI's Department of Societal Security and Safety. His background is in technical risk analysis and he works with methods development within the Swedish crisis preparedness system, often with a focus on risk and vulnerability analyses and critical infrastructure. He is active in the rebuilding of the new total defence.

Elin Hellquist is a senior analyst with a focus on international military operations, in FOI's Department of Operational support. She is one of the editors of Strategic Outlook 9. She has a doctorate in political science from the European University Institute, in Florence, and has long experience of security policy research.

Markus Henriksson is a senior scientist in FOI's Department of Electrooptical Systems. He has a doctorate in laser physics from KTH Royal Institute of Technology. He conducts research on, among other things, laser-based countermeasures, lidar sensors and laser dispersion in the atmosphere.

Jenny Ingemarsdotter is a scientist in FOI's Department of Societal Security and Safety, and focuses on crisis preparedness, civil defence and total defence. She has a degree in civil engineering and a doctorate in history of science and ideas, both from Uppsala University. Currently, she is engaged in a research project on civil defence in the grey zone. Jenny's research interests are broad and cover the history of total defence as well as ethical perspectives on artificial intelligence.

Ove Jansson is a cognitive scientist conducting research in FOI's Department of Man - Technology - Organisation. He works with questions involving human thinking and behaviour on different levels, from interface development of personal systems to methods development for conducting activity analyses. In addition to working with human optimisation equipment, he has also worked on questions dealing with autonomous vehicles, simulation environments and game systems, as well as selection and recruitment.

Fredrik Johansson is a senior scientist in FOI's Department of Decision Support Systems. He has a doctorate in technology (computer science) from Örebro University and conducts research on applications of artificial intelligence within defence and security, focusing on tools for intelligence analysis. Apart from his years of research experience at FOI, Fredrik has also worked operationally, with analysis of large data sets and method development in the Swedish Security Service.

Göran Kindvall is a senior analyst in FOI's Department of Strategy and Policy. He has a degree in civil engineering (technical physics) and a master's in technology (atomic and molecular physics). His primary tasks are long-term planning, technology evaluation and exploration of new concepts. In recent years, he has mostly worked with defence consequences of ongoing and future technology development.

Anders Larsson is a research engineer in FOI's Department of Hazard Protection, where, among other things, he works with indication methods for chemical and biological substances, as well as in CBRN-related questions in crisis preparedness and threats.

Britta Levin is a senior scientist in FOI's Department of Man - Technology - Organisation. She works with questions that involve the interaction between humans and systems, from a broad perspective. Her areas of expertise include measurement and valuation of human performance, methods development and simulation. Britta has a degree in aeronautical engineering from KTH Royal Institute of Technology, but is active in both aeronautical and land-based arenas, which in recent years has been directed at soldier systems, in both a national and international context.

Birgitta Liljedahl is a senior scientist in FOI's Department of Hazard Protection. She works with questions that involve CBRN, health and environment issues, in crisis and conflict. Currently, her focus is on elaboration of robust tools and scenario development, in part with VR modules, for complex CBR events in hybrid contexts, where uncertainty prevails about whether an incident is an accident, or antagonistic.

Sandra Lindström is a senior scientist in FOI's Department of Aerospace Engineering. She leads and coordinates the work focusing on space for defence and security. Her expertise is in global trends analysis with an emphasis on space, which includes global space development in the area of both technology and policy, as well as in the risks, threats and opportunities this creates for Sweden's defence and security. Sandra has a degree in civil engineering (space technology) from Luleå University of Technology.

Jenny Lundén is project leader and editor of Strategic Outlook 9. She is an analyst in FOI's Department of Strategy and Policy, with a focus on total defence. She has a master's degree in physics from Lund University and a doctorate in meteorology, with a focus on the Arctic, from Stockholm University.

Anders Melander is assistant project leader and editor of Strategic Outlook 9. Among other things, he has a master's degree in microbiology from Uppsala University. He is an analyst in FOI's Department of Strategy and Policy, with a focus on civil defence and total defence.

Karin Mossberg Sonnek has a doctorate in technology and is a deputy research director in FOI's Department of Societal Security and Safety. She has conducted research in climate adaptation, with a focus on municipal decision-making. In addition, she has studied the effects of climate change on societal activities, in research commissioned by the Swedish Civil Contingencies Agency (MSB), the Swedish Food Agency and SIDA, Sweden's government agency for development cooperation.

Björn Ottosson is a scientist in FOI's Department of Security Policy and Strategic Studies, with the USA as his expert area. He is one of the editors of Strategic Outlook 9. His primary analysis and study areas include American foreign, security and defence policy, as well as transatlantic relations. Björn has a doctorate in political science from Stockholm University and has worked previously at Stockholm University, Södertörn University and the Swedish Defence University.

Magnus Rosell is a scientist in FOI's Department of Decision Support Systems. He works with methods in machine learning and artificial intelligence, with a focus on tools for intelligence analysis, and leads projects on these themes. Magnus has a doctorate from KTH Royal Institute of Technology, in computer science. His dissertation deals with automatic text analysis and he has also developed methods for automatic global trend monitoring at the cybersecurity company, Recorded Future.

Niklas H. Rossbach is a senior scientist in FOI's Department of Security Policy and Safety, and conducts analysis of American and European security policy, energy and geopolitics, as well as the will to defend. He is also project leader for long-term global trends analysis. He has a doctorate in history from the European University Institute (EUI), in Florence, on the topic of transatlantic relations, and has done research on psychological defence at the University of Oxford.

Riitta Räty is a deputy research director in FOI's Department of Strategy and Policy. She has a doctorate in physics and works with the Armed Forces' capability development and futures research, including the Perspectives Study, as well as societal threats and risks, for various government authorities. Her interests included operations analysis, facilitation and workshops, futures studies and uncertainties.

K. Jack Riley is vice president and director of the National Security Research Division at the RAND Corporation. He leads a team of professionals who collectively conduct over 300 projects and produce hundreds of publicly available reports each year for top leadership in the national security community. As a researcher at RAND, he has led and co-led numerous projects on national and homeland security topics. Prior to joining RAND, Riley worked as a senior civil servant at the U.S. Department of Justice. Riley has a Ph.D. in public policy analysis from Pardee RAND Graduate School, an M.S. in foreign service from Georgetown University, and a B.A. in economics and Russian from the University of Michigan.

Lars Sjökvist is research director in laser technologies in FOI's Department of Electrooptical Systems at FOI. He is also a assosiate professor in chemical physics at Linköping University and has previously worked with magnetic resonance methods. His current research is directed towards military and security applications where different types of laser sensors and laser systems are used.

Liselotte Steen works in FOI's Department for Capability development. She is one of the editors of Strategic Outlook 9. She is an operations analyst seconded to the Navy Staff; her primary task is to support studies of navy systems. She has an extensive background at FOI and, before that, at the Swedish Armed Forces Materiel Administration (FMV). She has a degree as a high school teacher in science subjects.

Niclas Stensbäck is a computer scientist who conducts research in FOI's Department of Systems Technology. He leads a project in weapons system evaluation and general systems analysis. He has worked in several research projects involving autonomous systems, both as a developer of behavioural models and for assessment of future technical capabilities.

Anders Strindberg is a senior scientist in FOI's Department of Asymmetric threats. He is also an editor of Strategic Outlook 9. He works mainly with questions related to terrorism and violent extremism. He has a doctorate in international relations from the University of St Andrews, Scotland, as well as degrees in philosophy and theology. He also teaches in the master's programme at the Center for Homeland Defense and Security, U.S. Naval Postgraduate School, in Monterey, California.

Erik Svensson is an analyst in FOI's Department of Asymmetric threats. Erik's background is in peace and conflict studies and in political science, with a focus on crisis management. He has mainly worked on questions of cybersecurity, the effects of future technologies on military control, and provided analytical support to the Armed Forces and its study activities.

Gabrielle Tarini is a policy analyst at the RAND Corporation. Her research areas of interest include security cooperation, the NATO alliance, European security, and humanitarian and civilian security issues. Previously, she was a fellow in the Office of the Secretary of Defense for Policy and a research associate at the James Martin Center for Nonproliferation Studies. She has an M.P.P. from the Kennedy School of Government at Harvard University and a B.A. in international studies from Boston College.

Annica Waleij is a senior analyst in FOI's Department of Hazard Protection. Her research has primarily focused on health and environmental risks in international missions. Her international experience includes work in UN peacekeeping missions and being seconded to the UN's office for humanitarian issues, in Geneva. She has carried out field trips in Africa, where among other things she conducted environment and health investigations and trained UN and ECOWAS personnel.

Christoffer Wedebrand has a bachelor's degree in theology, with a focus on ethics, and a master's in peace and conflict studies. He is an analyst in FOI's Department of Societal Security and Safety, where his studies are primarily focused on peacetime crisis preparedness and the civilian aspects of total defence.

Per Wikman-Svahn is a researcher in the Department of Philosophy at KTH Royal Institute of Technology, Stockholm, where he conducts research on philosophical aspects of risk and uncertainty and teaches risk philosophy, research ethics and technology, and ethics, among other things. Previously, Per also worked at FOI, in the Defence Analysis Division.

Ann Ödlund is a senior scientist in FOI's Department of Strategy and Policy. Her background is in education, within behavioural science and organisational psychology. She conducts studies primarily in total defence, both from military and civilian perspectives, and has published several reports on the topic.

FOI

ISSN 1650-1942

www.foi.se