The Swedish Security Service

2022–2023

Sweden's independence and our democracy are values that may sound obvious and that we often take for granted. However, they are being challenged every day.

Charlotte von Essen, Head of the Swedish Security Service

The Swedish Security Service 2022/2023

Resilience in a troubled international climate

Russia poses a serious threat to the security of Sweden, and its actions, along with those of other authoritarian states, have become increasingly aggressive. In addition, and due to the troubled international climate, extremism is growing, the attack threat has increased, and the scope of the constitutional threat has widened. The remit of protecting national security has never been more important.

In the past year, the security situation has deteriorated significantly. This has had a direct effect on Sweden, as the external threat to Sweden affects our country's domestic security. Current global developments are difficult to assess; each threat adds to the overall threat, and changes occur quickly. The threat accelerates when the agendas of foreign powers and violent extremists coincide.

Tensions between the Russian regime and western democracies are increasing, and matters of national security have to be regarded in light of the fact that Russia views Sweden as a part of Europe and of NATO. What Russia will do next is unpredictable – the Russian regime has a tendency to take great risks. We can expect an increase in Russian intelligence activities and Russian activities that threaten the security of Sweden. This could, for example, be a matter of preparing to carry out sabotage, spreading disinformation, or using violent extremists in order to destabilise Sweden.

The intelligence and security-threatening activities of foreign powers are always ongoing. The main threat is currently posed by Russia. However, China and Iran, among other countries, carry out extensive and systematic espionage activities, procure technology, and gather information about and attempt to exert influence on individuals in Sweden who their regimes regard as threatening. China poses a growing and long-term threat.

The Swedish Security Service has in the past few years noted that actions by authoritarian states have become increasingly offensive. They use any means to achieve their goals. They are aggressive and use whatever resources they have at their disposal. The threat is further affected by the fact that authoritarian states have increased their cooperation in order to strengthen their own countries.

The situation after Russia began its war of aggression on Ukraine has affected and will continue to affect the security of Europe, including Sweden, for many years to come. Therefore, it has become more important for Sweden to have resilience and a well-functioning total defence system.

The Swedish Security Service, as a national ›

Charlotte von Essen,
Head of the Swedish
Security Service

The deteriorated security situation has had a direct effect on Sweden, as the external threat to Sweden affects our country's domestic security. Current global developments are difficult to assess; each threat adds to the overall threat, and changes occur quickly.

security service, is an important part of civil defence. Our Service's remit is to protect Sweden's national security and its democracy. The Swedish Security Service carries out both intelligence and security work – it should gather relevant intelligence and act on it in order to prevent and avert threats to Sweden's security and democracy. The Swedish Security Service is responsible for ensuring that what must not happen does not happen.

The altered security situation emphases the importance of building up the resilience of Sweden as a nation. An essential aspect of this is protecting our secrets, i.e. our most critical assets. Sweden is regarded as an attractive target by foreign powers wishing to fulfil their increased needs for technology, information and expertise. We must therefore increase our efforts within several sectors to protect them against espionage and sabotage.

Foreign powers are constantly on the lookout for weaknesses. This could be a matter of anything from taking advantage of vulnerabilities in IT systems or loopholes in Swedish legislation to carrying out crimes against life and health. It could also be a matter of deliberately increasing antagonism between certain groups in Sweden.

There are many possible ways to make a country weaker. Creating divisions is one of them. Another is by threatening and directing hatred at those who represent Sweden, e.g. politicians and journalists.

The Swedish Security Service has noted that current developments have led to increased extremism and have increased the constitutional threat. Mistrust in those who are perceived to have created the problems in Sweden has resulted in a polarisation that has led to an increase in extremism, which could also affect the attack threat. The line between extremism and violent extremism is becoming increasingly unclear.

Conspiracy theories and anti-state rhetoric that is very similar to violent extremist ideology is being spread on online platforms. This could undermine trust in the institutions of society, politicians' decisions, and the legitimacy of Sweden as a state. This situation is concerning, as it is being taken advantage of by both violent extremists and certain foreign powers. We have also noted some consequences of subversive activities in the past few years, for example the attack on the US Capitol and the incidents in Brazil and Germany.

We must work together to protect our fundamental democratic values. If fewer people stand up for democracy, this could lead to a decrease in resilience and the willingness to defend our country, which would play into the hands of certain foreign powers. Along with this, the attack threat posed by violent extremists remains. This can be noted not least in the events that have unfolded as a result of protests such as the January 2023 Quran burnings in Stockholm, resulting in an increased threat to Sweden and Swedish interests. Describing Sweden as an anti-Islamic country and trying to influence its possibilities of joining NATO

is an example of what can happen when agendas and interests coincide. The attack threat is also affected by the continued online radicalisation of potential lone attackers with an unclear ideology, sometimes underage, and sometimes suffering from mental health problems.

Taken together, these factors challenge the security of Sweden. As a security service, we closely monitor developments and changes in Sweden and internationally.

We take ongoing measures to protect Sweden and ensure the future of our democracy. However, detecting unknown threats before they are realised is an ever-increasing challenge as the volume of information increases. Being able to use the possibilities that technology has to offer, and having the right information at the right time, is therefore absolutely crucial to our continued ability to prevent terrorist attacks and espionage. In this work, our own technological capability is also important, and we work closely with our technology department when carrying out our operational work.

The work of the Swedish Security Service involves being one step ahead in order to counter the actors who want to harm Sweden and our democracy in various ways. We work in close cooperation with our national partners – such as the National Defence Radio Establishment, the Military Intelligence and Security Service, the Prosecution Authority, and the Swedish Police Authority – as well as with our international partners. In the last year, cooperation has been absolutely crucial to achieving success in this work, as well as to ensuring a safe and secure election, creating the conditions necessary for Sweden's EU presidency, and to achieving success in investigations into suspected offences against Sweden's national security. Cooperation with the other government agencies that make up the National Cyber Security Centre (NCSC) is a valuable aspect of protecting Sweden against a threat that is subject to change, as is the case in the cyber arena.

Sweden's independence and our democracy are values that may sound obvious and that we often take for granted. However, they are being challenged every day. The remit of the Swedish Security Service to protect Sweden's national security and its democracy has never been more important than it is now. ■

Charlotte von Essen, Head of the Swedish Security Service

Sweden as a nation must build up the resilience. An essential aspect of this is protecting our secrets, i.e. our most critical assets. Sweden is regarded as an attractive target by foreign powers wishing to fulfil their increased needs for technology, information and expertise.

Threats and vulnerabilities that affect Sweden's national security

Authoritarian states are strengthening their positions

Certain foreign powers pose a high threat to Sweden's security. Not only Russia, but also China and Iran, still pose the greatest threat in this regard. In recent years, authoritarian states have engaged in increasingly offensive activities. They are aggressive and use every resource available. The threat is further affected by the increased cooperation between authoritarian states.

Threats from certain foreign powers in the short and long term

Russia poses the greatest threat to Sweden. Russia's actions cannot be predicted, and its regime has a tendency to take great risks. Russia has the capability to carry out attacks and to engage in sabotage. China too poses an increasing and long-term threat to Sweden. In addition, Iran poses a tangible threat to the security of Sweden.

Risk that Sweden's total defence capability will be compromised

Vulnerabilities are increasing due to the rapid development of technology and the building up of Sweden's total defence. An increasing number of entities fall within the scope of Sweden's national security. Due to shortcomings in protective security however, Sweden's total defence capability risks being compromised while it is being built up. Protective security measures are meant to be a barrier against attacks.

A shifting threat that is subject to change

Security-threatening activities are being carried out on an ongoing basis by foreign powers through e.g. unlawful intelligence activities, influence operations, and cyber attacks. Due to the concerning global situation, the threat is subject to change, because there could be quick shifts in foreign powers' modus operandi and choice of targets, especially in the cyber arena.

Security-threatening procurement of technology

Certain foreign powers place extensive resources into procuring advanced technology in Sweden. One of the consequences of the current global situation and the war in Ukraine is that this has increased Russia's need for technology in order to maintain its military capability. China and Iran as well are engaged in extensive procurement of technology and expertise, for example in the area of research.

Attack threats and radicalisation

Recent developments have resulted in an increased attack threat. In addition, the extent of extremism is wide, fuelling violent extremism and affecting the attack threat. Potential attackers – often with unclear ideological motives, sometimes suffering from mental problems, and sometimes underage – are being radicalised online.

Increased threat to democracy

The threat associated with subversive activities has increased due to current developments. The spread of conspiracy theories and anti-government rhetoric is increasing, due to the efforts of both violent extremists and certain foreign powers. This could undermine trust in the institutions of society, politicians' decisions, and the legitimacy of Sweden as a democratic system.

Trust in the governance of Sweden is being undermined

Violent extremists are spreading encouragement to infiltrate or gain influence over various functional areas in Sweden. One of the aims of this could be to increase their own capability; another could be to affect decisions made by government authorities. Encouragement of infiltration could also be a way in the long term to undermine trust in the governance of Sweden.

A deteriorati in the inter situation

The greatly deteriorated international situation means that foreign powers present a high threat and that security-threatening activities are constantly going on. This development also poses a broader constitutional threat.


on
national

Situation report – Counter-intelligence

A changing threat as foreign powers become increasingly aggressive

Antagonism between the superpowers continues to increase and the prevailing world order is faltering. Sweden's security is at greater risk due to Russia's war of aggression against Ukraine and increased aggression on the part of other authoritarian states.

Security-threatening activities targeting Sweden — including intelligence gathering, influence operations and cyberattacks — are a daily occurrence. The threat posed by foreign powers remains high. The Swedish Security Service has noted a changing threat over recent years, as authoritarian states have become increasingly offensive as they attempt to consolidate their positions. Sweden is an arena for a conflict on a wider scale. As a whole, the Swedish Security Service notes that the sharply deteriorating international developments raise the risk to the security of Sweden.

"We can see that the situation has escalated and the stakes are higher. Foreign powers use all available means and all of the resources available in their societies to achieve their goals. So, the threat to Sweden is increasing and the potential consequences are very serious," says Henrik Edwinsson, a senior analyst with the Swedish Security Service.

To some extent, international developments have changed the nature of the threat; Russia now poses both a military threat in Sweden's vicinity and a threat to Sweden's internal security. Russia sees Sweden as part of Europe, of the West and of NATO.

"Russia is becoming more unpredictable and less risk-averse. The Russian central leadership has

> *We can see that the situation has escalated and the stakes are higher. Foreign powers use all available means and all of the resources available in their societies to achieve their goals. So, the threat to Sweden is increasing and the potential consequences are very serious.*
>
> *Henrik Edwinsson, Senior analyst with the Swedish Security Service*

also shown no aversion to using extensive violence to achieve its aims. The war of aggression against Ukraine also has a broader dimension in that Russia considers itself to be in conflict with the collective West and with NATO. In addition, the United States and Europe, including Sweden, have supported Ukraine in various ways, and this affects the threat," says Henrik Edwinsson.

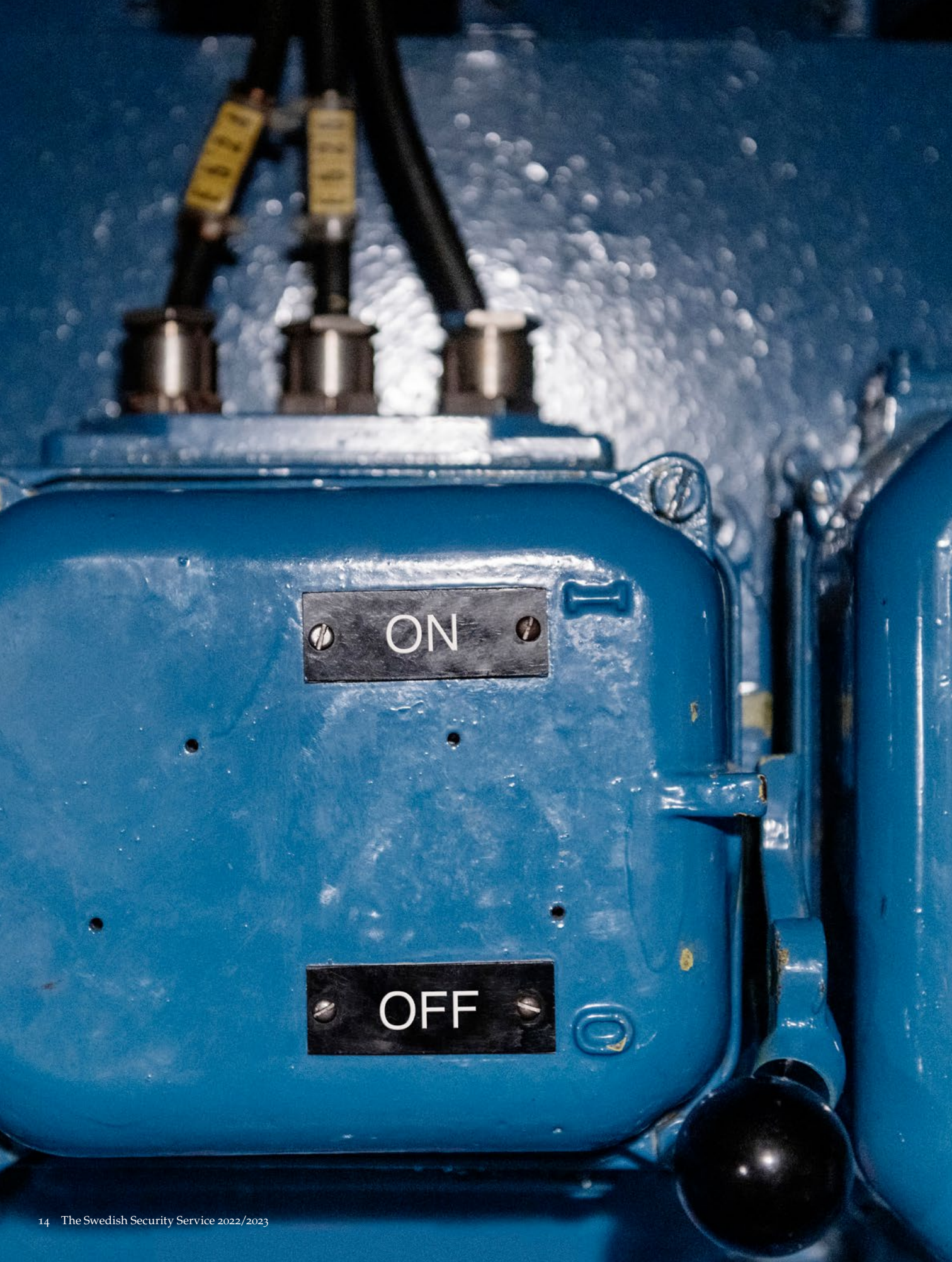
The changing nature of the threat Russia poses to Sweden may be manifested in various ways, such as through cyberattacks and disinformation. The Swedish Security Service also sees a development where Russia and other authoritarian states are cooperating with one another to a greater extent, for example to circumvent sanctions, which presents a challenge not only to Sweden but also internationally.

"If we are to make Sweden resilient, we cannot regard Sweden in isolation; rather, we need to build security with others, both nationally and internationally. Meanwhile, the threat is becoming increasingly complex as authoritarian states cooperate to a greater extent than previously, possibly affecting the overall threat to Sweden," says Henrik Edwinsson.

Foreign powers are greatly interested in Swedish research and industry and Sweden is at the forefront in many areas linked to military capabilities. The Swedish Security Service notes that the procurement of technology is becoming increasingly important to Russia, China and Iran. To this end, these countries and others are involved in ongoing covert procurement of technology and expertise aimed at increasing their own capabilities.

"The procurement of technology by foreign powers is a major problem. The international situation and the war in Ukraine have left Russia with an increasing need to acquire the technology required to maintain its military capabilities, but even China is highly involved in the covert procurement of technology and expertise," says Henrik Edwinsson.

Measures taken by the West have made it more difficult for Russia to gather intelligence or engage in security-threatening activities via official platforms. Russia might therefore use proxies in the form of companies or institutions to influence Swedish public opinion and Swedish policymakers or to obtain information. This could also involve using people in violent extremist environments to undermine and destabilise society, through for example disinformation or sabotage. ›


ON
OFF

While Russia is a clear threat to Swedish security here and now, China represents a more long-term and growing threat. China's overarching objective is to ensure the survival of the regime, and this is also the purpose of security-threatening activities targeted at Sweden. China uses its security and intelligence services to benefit Chinese interests in areas such as politics, economics, science and technology. Chinese citizens also have a legal obligation to assist intelligence services as and when necessary. China conducts multifaceted and qualified activities against targets in other countries. This includes Sweden and Swedish interests abroad.

Building a strong, rich and independent China demands cutting-edge technology, innovation and the development of military capabilities. To this end, Chinese actors in both the private and public sectors target Swedish businesses, the Swedish defence and space industries, and Swedish research institutes and higher education institutions.

Swedish technology, products, knowledge and data are assessed to be highly valuable to China's military development. Chinese investments and acquisitions in Sweden have increased sharply over the last decade in sectors where Sweden has cutting-edge expertise. As a consequence of this extensive Chinese activity against Swedish companies and research institutes, there is a risk that Sweden will be drained of innovation and competitiveness.

"While neither the acquisition of technology and expertise nor the influence operations conducted by the Chinese state in Sweden are necessarily always unlawful, they constitute a threat to Sweden's security. There still is a relatively widespread ignorance of the Chinese threat in Sweden, and this is in itself a vulnerability. This leaves Swedes in all societal functions and Swedish companies vulnerable to Chinese influence, intelligence gathering, and procurement," says Henrik Edwinsson.

For authoritarian states such as Russia, China and Iran, regime survival is the highest priority. Since the autumn of 2022, mass demonstrations have been taking place in Iran, leaving the regime focusing on domestic issues. That said, Iranian intelligence agencies have a long history of operating outside their own borders and, should pressure on the regime increase further, so too will the threat against dissidents in exile.

Iranian intelligence services pose a security threat to Sweden by conducting illegal intelligence operations, primarily targeting dissidents residing here. The Iranian regime gathers intelligence in Sweden and there is also a tangible threat of violence against dissidents worldwide. Given the large Iranian diaspora in Sweden, many of whom exercise their constitutional right to criticise the Iranian regime, Iranian intelligence and security agencies clearly have an interest in monitoring and gathering information about such people in Sweden.

In a troubled world in which foreign powers act in an increasingly aggressive and unpredictable manner, the situation has also become increasingly insecure for Sweden.

"In the last year, we have noted interstate conflicts and even protests and increasing discontent in many authoritarian states. This development increases the risk of these regimes behaving in an unpredictable manner, which causes uncertainties and makes it difficult to assess the situation as a whole and its likely impact on Sweden," says Henrik Edwinsson. ■

Summary – Counter-intelligence

The Swedish Security Service notes that the threat to Sweden has changed. Russia and other authoritarian states are acting more aggressively and cooperating with one another, increasing the risk to Swedish security. The three countries that present the greatest security threat are Russia, China and Iran. The unlawful procurement of technology by foreign powers is a major problem.

Situation report – Protective security

The gap between threat and protection creates vulnerabilities

The international situation has created a changeable threat where the targets of foreign powers are subject to quickly change. Together with the general lack of awareness by organisations and entities about what they should protect, this situation could result in vulnerabilities.

Protective security must be designed to deal with a changing threat. Russia's war of aggression against Ukraine has international consequences, which, in turn, alter the threat. The approaches and targets chosen by foreign powers may shift rapidly based on developing events, especially in the cyber arena. Organisations therefore need to continuously test and evaluate their own protective security.

Due to the deteriorating security situation, the rebuilding of Sweden's total defence has become increasingly imperative to national security. Both public-sector and private-sector organisations have a key role to play in this rebuilding. In conjunction with this, more actors will have acquired expanded or new tasks and roles of significance to Sweden's security that therefore demand adequate protective security.

The rebuilding of the total defence means that more organisations conduct security-sensitive operations. This in turn increases risks, as organisations that did not previously have access to sensitive information now need to process it in a secure manner. Here, the Swedish Security Service can see shortcomings.

"Protective security should constitute a threshold for attack. It is therefore a matter for concern that there are shortcomings in organisations' protective security work. If security protection is flawed, there is a risk that Sweden's total defence capabilities will be revealed as they are built up," says David Hughes,

The approaches and targets chosen by foreign powers may shift rapidly based on developing events, especially in the cyber arena.

David Hughes, in the Swedish Security Service's Protective Security Unit

Summary – protective security

Foreign powers constantly take action meant to create uncertainty and exert pressure. There are shortcomings in the ability of organisations to protect themselves against both espionage and sabotage. Organisations also lack knowledge of what critical assets they have. This, together with shortcomings in their security protection, risks revealing Sweden's total defence capabilities.

in the Swedish Security Service's Protective Security Unit.

For security-sensitive organisations, there are currently shortcomings in all areas of protective security, i.e., personal, physical and information security. Among other things, there are shortcomings in organisations' ability to detect breaches in information systems and there are fundamental shortcomings in areas such as the protective security analyses that they are obliged to perform. There are also shortcomings in procuring goods and services that are subject to protective security agreements.

Meanwhile, the Swedish Security Service notes that international developments are making it difficult for organisations to judge what constitutes a security-sensitive operation. In combination with an inability to identify critical information and activities, this creates vulnerabilities. Although there is uncertainty about what should be classified as a security-sensitive operation, there is a greater awareness of the importance of protecting it.

"There is a greater understanding and awareness that a threat exists. While there is still a gap between protective security and our adversaries' capabilities, the conditions will be created to at least lessen this gap as awareness increases. Many organisations are working intensively to improve this area but lack of resources and skills presents a real problem," explains David Hughes.

The Swedish Security Service issued warnings to organisations on several occasions in 2022 urging them to strengthen their protective security and increase vigilance due to the deteriorating international situation. These warnings were specifically aimed at sectors where an attack is particularly likely to cause particularly great damage to Sweden's security and in some cases to the security of Europe and the West.

These warnings led to a sharp increase in the number of incidents reported.

"Foreign powers constantly take action meant to create uncertainty and exert pressure. In light of current world events, it is vital that security-sensitive operations are subject to increased vigilance. It is our joint responsibility to keep Sweden secure," says David Hughes. ■

Situation report – Counter-terrorism

The threat to democracy when confidence in society is undermined

International developments pose a significant threat to Sweden and the democratic system. Violent extremists and foreign powers alike are working to destabilise society. Meanwhile, there is an elevated threat of attack.

The deteriorating global security situation has an impact on the violent extremist environments monitored by the Swedish Security Service, which use and react to international events as proof of a supposedly negative societal development and as a justification for taking action to rectify the situation. These actors utilise a variety of methods aimed at a range of targets.

"While the threat of traditional terrorists attacks persists, the broader threat to democracy is becoming increasingly prominent. Violent extremists use the same subversive methods as foreign powers, including infiltration and influence, to widen divisions in society," says Fredrik Hallström, Head of Counter-terrorism and Counter-subversion at the Swedish Security Service.

The traditional threat is primarily posed by lone actors motivated by violent Islamist or violent right-wing extremism. The threat level can quickly change, as demonstrated by events such as the burning of the Quran outside the Turkish Embassy in Stockholm in January 2023. In the intelligence flow, the Swedish Security Service notes an increasing number of threats against Sweden and Swedish interests abroad as Sweden becomes the focus of violent Islamist extremism. This turn of events also benefits foreign powers and has an impact on violent right-wing extremism.

Regardless of ideological motivation, opposition to the state, society and its representatives has always been a pillar of violent extremism. While the remit of the Swedish Security Service relates to the security threat posed by violent extremists, this threat is not currently limited to criminal acts alone. The Swedish Security Service has noted a shift from the straightforward threat of attacks to a broader type of threat to society.

"There are many ways to weaken the democratic society in order to undermine confidence in society in the short and long term, and far from all of these ways are covered by the Criminal Code," says Fredrik Hallström.

Such activities may involve disseminating disinformation that is often based on conspiracy theories concerning the illegitimacy and corruption of the state. Conspiracy theories are not confined to violent extremist environments. Extreme ideas and anti-establishment narratives have taken root in a broader stratum of society, something that is exploited by violent extremists as well as by foreign powers.

"Conspiracy theories are not criminal in themselves, and there has always been opposition to the

The most serious threat is not necessarily the acute threat to life and health. It may actually come from activities that are not in themselves unlawful but that are intended to covertly and quietly overturn society and our democracy.

Fredrik Hallström, Head of Counter-terrorism and Counter-subversion at the Swedish Security Service

establishment. However, conspiracy theories spread a narrative that may help to erode confidence in society and its institutions. This in turn may pose a threat to security. This was exemplified by the storming of the United States Capital Building in 2021 and the raids on the suspected coup plotters in Germany in 2022," says Fredrik Hallström.

The Swedish Security Service notes that violent extremists encourage sympathisers to infiltrate various parts of society, both in order to increase their own capabilities – in combat and weapons handling, for example – and to exert influence over policies and decisions. Incitement to infiltration may also be a matter of undermining confidence in society in the long term. Eventually, this may require a reassessment of the threat posed by violent extremism and how this can be countered.

"The most serious threat is not necessarily the acute threat to life and health. It may actually come from activities that are not in themselves unlawful but that are intended to covertly and quietly overturn society and our democracy. Discovering and countering this presents a major challenge to the Swedish Security Service," says Fredrik Hallström. ■

Summary – Counter-terrorism

International developments pose a significant threat to Sweden and the democratic system. The usual threat of attacks from violent Islamist and violent right-wing extremism remains and in some respects is increasing, while the broader threat to democracy is becoming increasingly prominent. Violent extremists carry out subversive activities in the form of infiltration and influence in order to increase divisions in society.

Subversive activities

Covert security-threatening activities aimed at overthrowing or changing the democratic system or making the country dependent on foreign powers. Subversive activities are conducted through, for example, propaganda, disinformation, infiltration, criminal activities, sabotage and terrorist threats.

Russia procures technology in Sweden to increase military capabilities

In November 2022, two Swedish citizens were arrested on suspicion of carrying out activities that pose a serious threat to Sweden and other countries. These individuals are suspected of having procured technology that Russia uses for military purposes.

The suspicions concern gross unlawful intelligence activities in the form of shipments of advanced technology with military applications – such as rockets, satellites and other weapons technology – to Russia and its military intelligence service, the GRU. These shipments allegedly went via the company that the pair run together. It is also suspected that they procured technology from the United States and sent it to Russia via Sweden.

The Swedish Security Service is running a preliminary investigation into this matter under the leadership of a prosecutor from the National Security Unit of the Swedish Prosecution Authority. At the time of writing, it remains to be determined whether it will be possible to file charges in this case.

Russia is in great need of advanced technology and expertise in order to develop and increase its capabilities. By covertly procuring technology, Russia is able to circumvent the sanctions that have been imposed in various rounds since the annexation of Crimea in 2014. Russia uses a variety of methods to gain possession of information from Sweden. Such methods include everything from strategic acquisitions to sending intelligence officers under diplomatic or other types of cover to recruit agents in Sweden. Russia also makes use of company organisational structures that are in themselves often legal but that make efforts to unlawfully procure technology with a view to sending it to Russia.

"Sweden is an attractive target for Russia, as we are at the forefront in areas of interest to Russia. We also have an open research and business culture that is favourable for countries like Russia to operate in. It is important that companies and researchers understand that technological products, such as semiconductors, used for civilian purposes also have military applications. Such technology, that Russia acquires unlawfully, is ultimately what it needs in order to wage war," explains Charlie*, who works in counter-intelligence at the Swedish Security Service.

Although the procurement of technology and expertise is always ongoing, Russia has become more active in this area in the last few years.

"It is a top priority of the Swedish Security Service and Sweden to counter and prevent Russia's procurement of technology in this area, in order to hinder Swedish technology from being used unlawfully in the war against Ukraine or any other states, and because such technology could be used to directly threaten the security of Sweden," says Charlie. ■

** This individual has been anonymised for security reasons.*

Lone terrorists are part of a complex threat

Those who plan and commit terrorist attacks or other serious crimes of violence on their own are part of a complex threat, and detecting such individuals poses a challenge to security services worldwide. An example is the preparation for terrorist offences and the resulting murder by a lone actor during the Almedalen Political Week.

There is no universally accepted definition of a lone terrorist, nor do they collectively constitute a homogeneous category of actors. Such actors may elect to operate on their own for a variety of reasons.

Historically, violent extremists have always adapted to changing conditions and circumstances. For example, as security services around the world have become more adept at detecting and gathering information about groups and organisations that may pose a threat to society, the number of lone actors has increased, one of the reasons being that it is easier to avoid detection by operating alone. Another factor behind an individual's choice to operate alone could be personal circumstances, such as physical isolation and difficulties in connecting with people socially.

Lone actors often focus on general objectives related to their personal convictions rather than the causes of particular organisations. That said, they often share convictions and a calling to "do something" with others, and see this as legitimising their actions. Collectively, these lone actors constitute a larger context found to an increasing extent on social media platforms, where their activities are difficult to detect, assess and counteract.

The Swedish Security Service is well-aware that lone actors interact on digital platforms with individuals who have ideologically convictions similar to their own and who are sometimes located far beyond Sweden's borders. On these platforms, they receive both instructions and manuals on how to procure weapons and make bombs, and they express their hatred of society or of specific groups.

Considering the interplay between ideology and

personal circumstances, the range of conceivable targets for lone actors who have the intent to cause harm to society is wide. Targets or victims are not always decided from the conceptual state or when various preparations are being made but could be decided when an opportunity arises.

In the reports received by the Swedish Security Service about certain individuals in this context, there are often indications of mental health problems. Many of these individuals are young. In addition, there are indications that violence in itself could be a motivating factor. The ideas of what is unjust and of who is responsible for what is regarded as negative developments in society are not infrequently based on various conspiracy theories. The common thread is the idea that society must be changed or even overthrown.

The man who, during the Almedalen Political Week in July 2022, murdered the national coordinator for psychiatry at the Swedish Association of Local Authorities and Regions, was a lone actor with no obvious affiliation to any ideologically oriented group. He was also charged with planning the murder of the leader of one of Sweden's political parties. The Stockholm District Court sentenced the man to institutional psychiatric care with special discharge review for murder and preparation to commit a terrorist offence, a judgement that is now final. ■

An investigation at the bottom of the sea

The suspected gross sabotage of the Nord Steam 1 and 2 gas pipelines has affected several countries. The Swedish Security Service is conducting a one-of-a-kind investigation into this matter. Cooperation is a key element in this investigation.

In late September 2022, gas began leaking into the Baltic Sea from both Nord Stream 1 and Nord Stream 2. Shortly after the leaks were detected, the Swedish Security Service took over the investigation, which is headed by a prosecutor from the National Security Unit of the Swedish Prosecution Authority. The Swedish Security Service took over the investigation because the case concerns a gross crime that, at least in part, could be targeting Swedish interests, and because the possibility that a foreign power could be behind the detonations could not be ruled out.

The incidents have had political repercussions in terms of both national security and energy-related concerns. The sabotage has affected several countries.

Well-functioning cooperation between Swedish public authorities has been vital to the investigation into this matter. While this cooperation has mainly taken place at a national level and between Swedish public agencies, the Swedish Security Service has also collaborated with other countries in this matter.

While conducting the two crime scene investigations, the Swedish Security Service received expert assistance from the Swedish Armed Forces, Swedish Coast Guard and Swedish Police Authority. In the investigation thus far, which is still ongoing, gross sabotage has been confirmed and traces of explosives have been secured. ■

Activities of powers

Countries such as Russia, China and Iran conduct security-threatening activities in and against Sweden, including espionage, cyberattacks, illegal procurement of technology and influence operations.

foreign in Sweden

How Russia, China and Iran are threatening Sweden's national security

Russia, China and Iran all conduct extensive intelligence gathering and security-threatening activities in Sweden that pose a threat to the country's territorial sovereignty and independent decision-making. These activities also undermine fundamental rights and freedoms, cause unemployment in and drain knowledge from Sweden.

Russia – the greatest threat

Russia is the single largest actor threatening Sweden's security and is assessed to be the only actor in Sweden's immediate vicinity that poses a military threat.

Russian intelligence and security services provide a toolkit for achieving the Russian regime's strategic objective of strengthening the country's geopolitical, technological and military position. Their mission also includes removing threats to the regime.

Russia gathers intelligence in Sweden on a continuous basis, including through Russian diplomatic missions in Sweden, where intelligence officers work under diplomatic cover to gather information on Swedish policy, defence and the economy. Some are also engaged in acquiring civilian and military technology.

Intelligence gathering is the main security-threatening activity conducted by Russia in and against Sweden. Targets include Swedish politicians and civil servants, the Swedish total defence, civilian and military industries and individuals residing in Sweden who are critical of the Russian regime.

Russia uses cyber-espionage and signals intelligence to gather intelligence from Russian soil. This technical intelligence gathering is methodological and long-term.

Russia is engaged in covertly procuring advanced technology and expertise, among other things to boost its own military capabilities.

Russia uses proxies to destabilise, establish platforms for influence operations, create sabotage capabilities and to prepare for war. It also uses legally dubious business front companies. Russia uses Sweden as a platform to increase its military capabilities.

Influence operations are among the security-threatening activities conducted by Russia in and against Sweden. While such operations primarily target members of the Russian diaspora in Sweden, influence is also exerted on politicians and civil servants. Russia also spreads disinformation in order to affect the image of Russia.

China – a growing long-term threat

Chinese intelligence agencies conduct extensive and systematic intelligence and security-threatening activities against Sweden and Swedish interests with the aim of achieving China's long-term ambition to position itself as a global superpower.

Chinese intelligence activities target a wide spectrum of Swedish society. From Sweden's viewpoint, the gravest intelligence threats are posed by Chinese intelligence officers, either travelling to Sweden or working from and within China, and Chinese computer network attacks.

China nurtures ambitions to become a global leader in several fields of technology, including space technology. Swedish technology, products, expertise and data are considered to be highly valuable to achieving China's long-term objectives. Chinese investment in Sweden has increased significantly over recent decades, both in sectors where Sweden has cutting-edge expertise and in critical infrastructure. This is done with the intention of procuring technology, innovations, expertise and personnel, and to access networks and development platforms in prioritised sectors, but also to influence Swedish policymakers. Chinese activities such as the strategic acquisition of companies, and the procurement of technology, particular products and expertise, may pose a serious threat to Sweden and Swedish interests.

Other Chinese activities, such as research and business exchanges, strategic product procurement, investments and acquisitions, and the transfer of technology and expertise via recruitment programmes may also constitute serious threats to Sweden's security. Such activities, besides enabling China to gather a great deal of information, also often give China access to sensitive information, expertise, products and technology.

China gathers information about dissidents living in Sweden and conducts extensive intelligence and threatening activities against critics of the regime for the purpose of limiting their freedom of expression and action. China also puts extensive resources into influencing international opinion and encouraging individuals to practice self-censorship, including in Sweden.

China has a high capability to carry out electronic attacks and uses cyberattacks to gather information.

China pursues a policy of influence designed to reshape global norms and values and to quench opinions critical of the Chinese regime. It also seeks to persuade other countries to make decisions that favour Chinese interests.

The Chinese National Intelligence Act of 2017 requires citizens to assist the Chinese intelligence services whenever necessary.

As a whole, Chinese security-threatening activities risk undermining Swedish innovation and exports which could eventually severely impact the competitiveness of Swedish industry and increase unemployment, and therefore pose a serious threat to Sweden.

Iran – a tangible security threat

Iran conducts security-threatening activities in Sweden and against Swedish interests, including intelligence gathering, influence operations against dissidents and through procurement activities. Iranian intelligence agencies also have a long history of carrying out attacks on individuals considered to pose a threat to the stability of the Iranian regime.

In Sweden, the primary targets of Iranian intelligence operations are dissidents in the Iranian diaspora.

It is common for people travelling to Iran to be approached by Iranian intelligence services. In recent years, the risk of being subjected to such approaches and of being arbitrarily detained has increased.

Iran has also shown an interest in cutting-edge Swedish technology and dual-use products with civil and military applications. Iran unlawfully acquires both technology and expertise, and uses Swedish higher education institutions to develop its own capabilities.

Iran also engages in industrial espionage, primarily targeting Swedish hi-tech industries and products that can be used in Iran's nuclear weapons programme.

In recent years, a number of cases in which Iranian intelligence agencies have planned or carried out attacks have garnered attention in Europe. This includes cases in Sweden where, for example, an individual was in 2019 convicted of serious unlawful intelligence activities against individuals. There have also been cases since then in which the Swedish Security Service has averted attacks linked to Iranian intelligence services.

Besides gathering intelligence via human sources, Iran also carries out computer network attacks as an intelligence gathering tool.

Vulnerabiliti digitised

The digitisation of society increases opportunities for foreign powers to gather intelligence and carry out disruptive attacks. Digitisation also enables violent extremists to reach more people and forge new alliances.


es in a
world

Violent extremism in a digital world

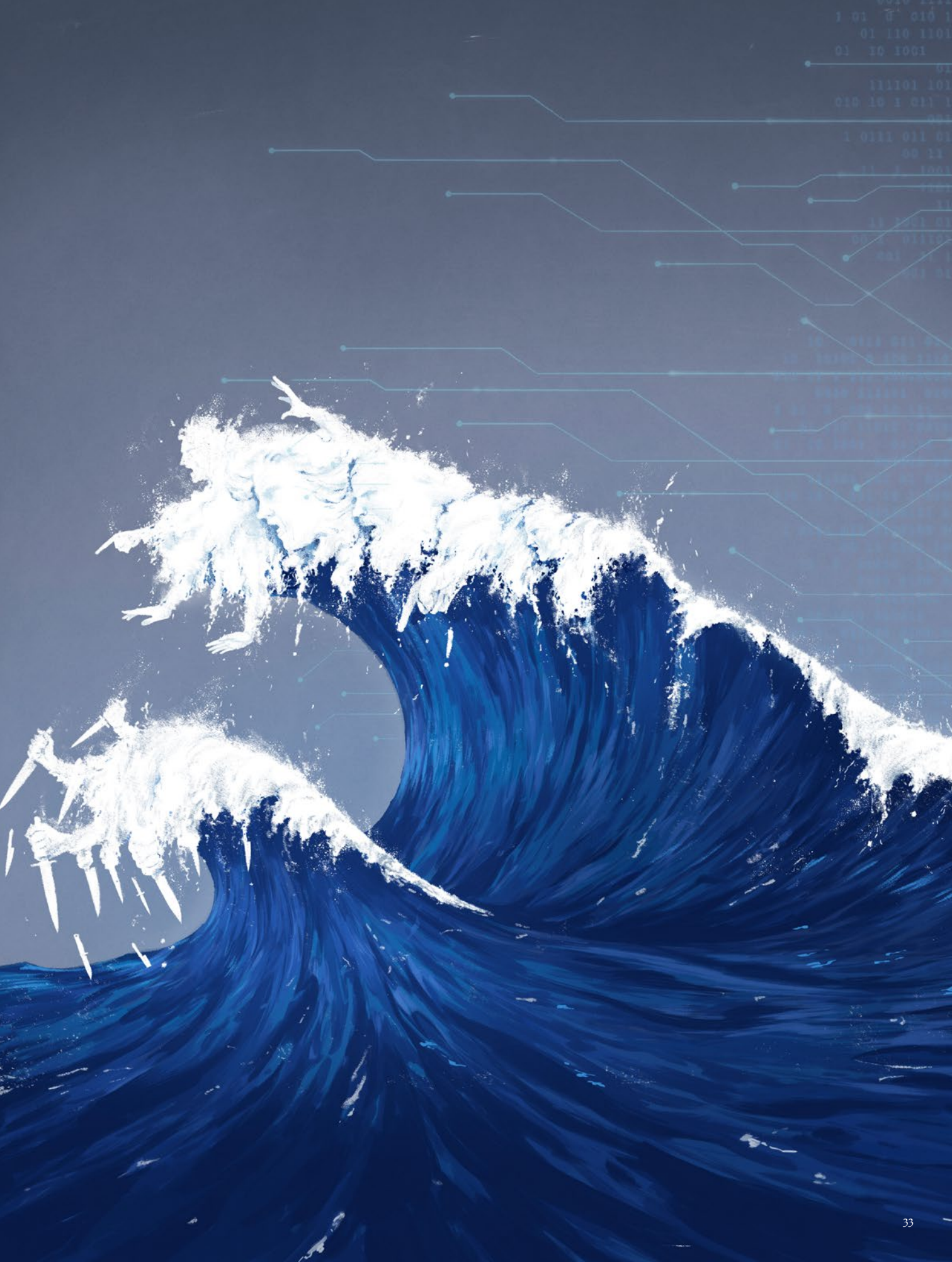
With digitisation, many of the activities of violent extremists have moved online. The internet is now home to both radicalisation and recruitment. This development makes it more difficult to detect threats.

The ongoing and long-standing digitisation of society affects the actors that the Swedish Security Service monitors. More and more people are now being reached by the rhetoric of violent extremists and the Swedish Security Service notes an increased tendency to dehumanise and legitimise violence.

This interaction primarily takes place on digital platforms. Opportunities to rapidly forge new alliances and reach others with the same worldview regardless of geographic location are underlying factors. This development can lower the threshold for engaging in violent extremist environments and committing criminal acts. Extreme thoughts and expressions have become normalised and, to some extent, acceptable.

"This makes it difficult to distinguish between violent extremists with the intent to commit acts to harm society and those simply expressing their opinions in an extreme manner, especially as those who propagate conspiracy theories and express hate and a negative view of societal development – and who may even encourage violence – are driving the radicalisation of violent extremists. Many of them spend a large part of their time in the digital world where there is a great risk that they will become trapped in an echo chamber that reinforces and encourages narratives and thought processes rather than challenging them," says Susanna Trehörning, the Swedish Security Service's Deputy Head of Counter-terrorism and Counter-Subversion.

Many of the lone actors that plan and execute terrorist attacks and other serious violent crimes are members of digital communities in which they interact with likeminded people from different parts of ›



Those who propagate conspiracy theories and express hate and a negative view of societal development – and who may even encourage violence – are driving the radicalisation of violent extremists. Many of them spend a large part of their time in the digital world where narratives and thought processes are reinforced and encouraged rather than challenged.

Susanna Trehörning, Swedish Security Service's Deputy Head of Counter-terrorism and Counter-Subversion

the world. This often takes place in encrypted areas of the internet where information is only accessible for a short time. This is presenting increasing challenges. The Swedish Security Service processes large amounts of data, a workload that increased further since the protests such as the burning of the Qur'an in Stockholm in January 2023. This is a trend that is expected to continue.

"Since the protests we have seen a very large increase in concrete terrorist attack threats. Meanwhile, the dissemination of hate and conspiracy theories continues," says Susanna Trehörning.

Digital development increases opportunities to operate covertly.

"This in turn implies that we can expect the number of unreported online threat actors to increase significantly. We therefore need the right tools to identify the threats, for example, the Swedish Security Service needs to be allowed to process data in a manner that increases our ability to both assess and prevent threats. We have also previously discussed the need to criminalise the possession of videos showing executions and torture, to curb a trend towards the normalisation of violence," says Susanna Trehörning.

The Swedish Security Service also notes that radicalised forces are disseminating their message through channels where young people spend their time, such as popular social media, and gaming and streaming platforms. It is not a new phenomenon to find violent extremists seeking out such places in an attempt to influence and recruit young people; violent extremists will be found where young people gather, whether in the digital or physical world.

"In part, this is because violent extremists have long-term objectives and therefore focus on recruiting youths, who they consider to be impressionable. But it is also because many violent extremists are young themselves and can interact with their peers on social media relatively undisturbed," explains Susanna Trehörning.

The Swedish Security Service has seen examples of young people having come into contact with people with strong ideological convictions from their bedrooms in the family home, receiving instructions and manuals on weapons and bomb-making and expressing hatred of society or of particular groups.

It can be difficult for outsiders to detect radicalisation, especially when it takes place digitally. Digital platforms also facilitate anonymity, which can make it difficult to determine who is behind the information or opinions being shared. Antidemocratic rhetoric that is often false may be hidden in a feed of otherwise accurate information. Threat actors package their rhetoric to suit a young target group. More often than not, they use words and images that are not in themselves unlawful, but that may contribute to instilling a sense of "us and them" at an early age.

The negative consequences of these actions are not only radicalisation but also hatred spread online, bullying, and harassment. This in turn may make young people more receptive to the violent extremist rhetoric.

"In our influx of information, we note many young people. It is therefore important that everyone in society helps and that adults and good role models are on hand to see and validate young people, so that the forces of evil do not gain a foothold. It is also vital to interrupt the echo-chamber effect that leaves radical opinions largely left unchallenged. This can be achieved, for example, through increased discussion. Everyone who interacts with young people can contribute to increasing the resilience to violent extremism," says Susanna Trehörning. ■

The flipside of the interconnected society

Large parts of society are increasingly dependent on digital technology for the day-to-day operation of large parts of our society. There is clearly a risk that cyberattacks designed to access, damage, disrupt or manipulate vital societal functions and systems will have an increasing impact. Organisations must be able to withstand such attacks, even in the worst of situations.

Digital development increases opportunities for foreign powers and criminal gangs to collect data and launch destructive attacks. Cyberattacks are a toolbox serving a multitude of purposes, such as advancing a country's foreign and security policy agendas, benefiting research and development in one's own country, creating competitive advantages for domestic companies or preparing covert influence operations. In some cases, cyberattacks are prepared far in advance for use in an escalating situation.

"Ultimately, cyberattacks can be utilised as part of an armed attack on a country by targeting vital societal functions and infrastructure. This is something we have seen in Ukraine over the past year. For criminal gangs, cyberattacks have increasingly become a tool for breaching and stealing sensitive data or installing ransomware that encrypts critical systems to extort money from the system's owner. This threat has increased, threatening to disable vital societal operations, including security-sensitive operations," says Nils Alenius, information security specialist with the Swedish Security Service.

A modern IT environment consists of a complex combination of systems, applications and connections, many of which are linked to online and cloud-based solutions. This exposes data and systems to the outside world and creates vulnerabilities and often intractable dependencies, including for organisations with security-sensitive operations. When a service provider has far-reaching access to critical systems, hardware or software, an attack against the supplier or supply chain may have disastrous consequences. >

An attack on a supplier or digital supply chain that, for example, succeeds in installing malware along with a software update can provide unauthorised access to multiple IT environments and may indirectly impact security-sensitive organisations without specifically targeting them. Dependence on components, software, services, competences and the digital chains that supply them creates vulnerabilities that may harm Sweden.

"Digitisation has many benefits and much of the digitisation that has taken place is necessary to maintaining an efficient and competitive modern society. Unfortunately, with digitisation comes a number of complex dependencies and vulnerabilities that have not always been adequately addressed. Deficiencies in the security work carried out by a supplier or partner – a missed security patch, for example – can have rapidly escalating consequences for the IT environment of one's own organisation. It is vital to practice comprehensive protective security management in order to protect oneself against the attacks that digitisation opens the way for," says Nils Alenius.

Certain types of system are continuously connected to the internet, making them vulnerable to malicious actions such as denial-of-service attacks, data breaches and even outright sabotage.

"We see that organisations often fail to conduct a sufficiently thorough review and evaluation of the pros and cons before acquiring or developing IT systems and services. At the end of the day, this means that the organisation as a whole – and in a worst-case scenario, the security-sensitive parts thereof – are vulnerable to the complex, unmanageable chains of dependency that digitisation entails," says Nils Alenius.

In the assessment of the Swedish Security Service, as societal functions, the financial sector and, ultimately, people's lives and health become linked to interconnected systems, there is clearly a risk that the consequences of cyberattacks will become increasingly severe. This threat will only increase as more or less advanced AI solutions are increasingly used to automate societal functions.

Regardless of who is behind the attacks, it is not enough to simply protect against attacks generally; organisations must be able to withstand worst-case scenario attacks. We are now seeing an escalation in the wider world, with cyberattacks having become a way to engage in warfare, which is clearly a worrying development.

Nils Alenius, information security specialist with the Swedish Security Service

"Technological advances may bring new vulnerabilities at the same time as they can reduce old ones, something exemplified by AI. The growing amounts of data in society and developments in the wider world mean that the Swedish Security Service must be better able to quickly collect, process, analyse and make available relevant information. We need to take full advantage of the opportunities offered by technology when it comes to processing data, including the use of AI, so that we can identify unknown threats before they can be realised," explains Nils Alenius.

Organisations all over Sweden are subjected to cyberattacks on a daily basis. These attacks, which may be orchestrated by foreign powers or criminal gangs, present a high level of threat. One clear trend is for criminals to create backdoors into systems that they can then sell to other interested parties, who in turn carry out cyberattacks such as the theft of valuable data or ransomware attacks.

Another development noted by the Swedish Security Service is that criminals are becoming increasingly strategic and farsighted when it comes to utilising information acquired in previous cyberattacks. There are examples of criminals using emails stolen in previous data breaches in new phishing attempts. This creates legitimacy; if the sender appears to work within the same organisation, it is more likely that someone will click on a malicious URL.

"Regardless of who is behind the attacks, it is not enough to simply protect against attacks generally; organisations must be able to withstand worst-case scenario attacks. We are now seeing an escalation in the wider world, with cyberattacks having become a way to engage in warfare, which is clearly a worrying development. When cyber-weapons are used in conflicts, there is also a risk that they will be aimed directly at Swedish targets, or that they will indirectly harm Swedish targets and interests through various global digital supply chains," says Nils Alenius. ■

Cyberattacks by foreign powers

Several countries carry out cyber-attacks against Sweden, often as part of a long-term agenda. The Swedish Security Service sees a tendency for states to use privately-owned infrastructure to launch attacks.

The more digitised society becomes and the more information becomes available digitally, the greater the opportunities for attackers to collect data via cyberattacks.

"That said, these actors do not carry out attacks solely to gather information. They also carry out attacks in order to build up their own infrastructure for the purpose of preparing for future attacks or gaining access to systems or methods that may prove useful later on," says Mia*, who works in counter-espionage at the Swedish Security Service.

While China is the main culprit when it comes to building up networks based largely on internet

Five phases of cyberattacks

Identification of vulnerabilities: The attacker identifies the vulnerabilities of a potential target, or of specific products, in preparation for future attacks.

Trial attempt: The attacker attempts to gain access to an IT system — for example, by embedding malware, through vulnerabilities in software or via spear phishing — for the purpose of taking advantage of the already identified vulnerabilities.

Access: Once the attacker has access to the system, they covertly attempt to increase their degree of access and establish permanent access. Access need not be utilised immediately but may lay dormant for a long time.

Data exfiltration: Work begins to exfiltrate data from the system. The attacker may choose to transfer data continuously over an extended period of time, or rapidly before leaving the system. Methodology depends on the nature of the intelligence mission.

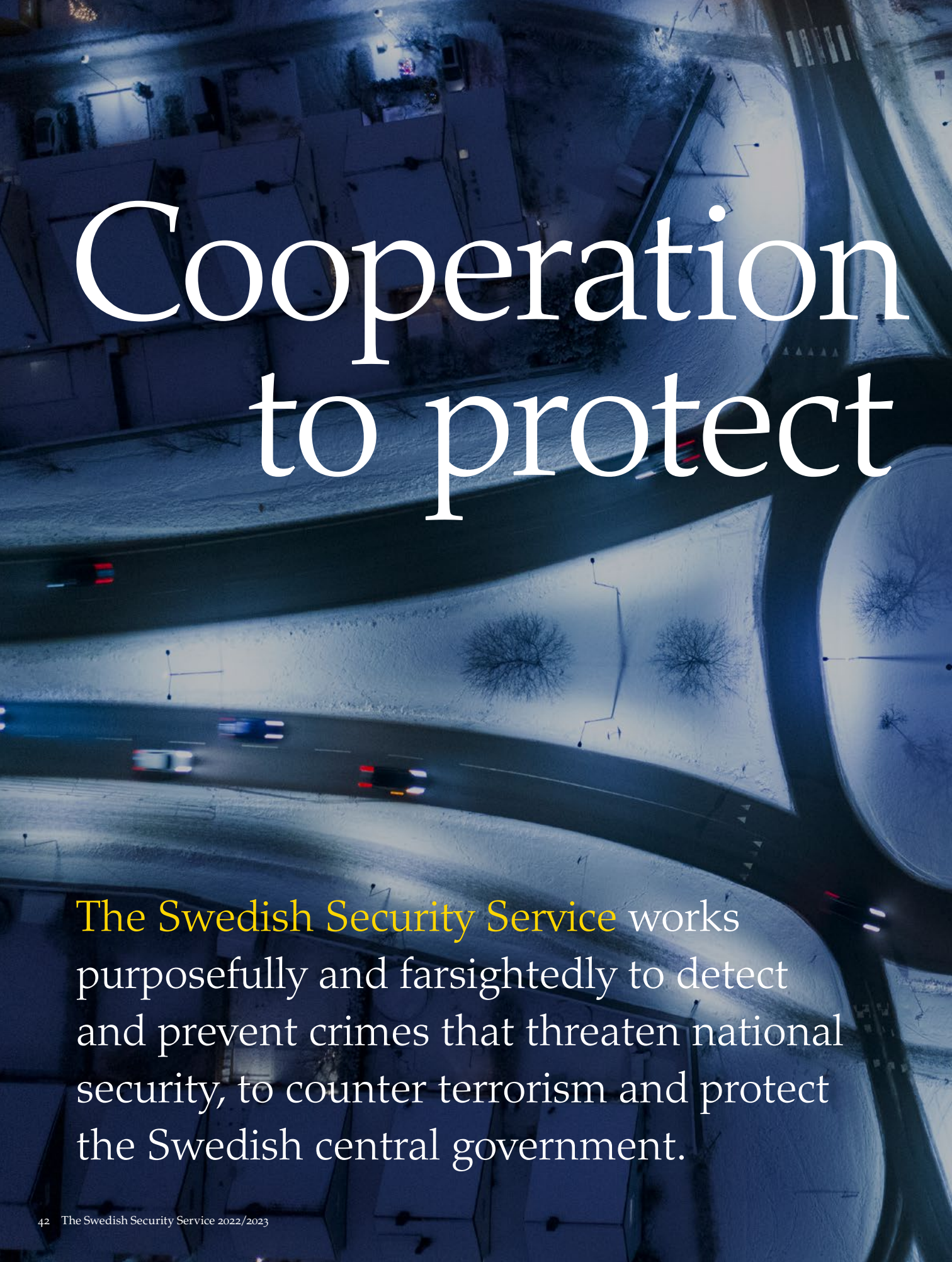
Sabotage: The attacker destroys data or prevents access to it so that the IT system cannot be used.

connected devices owned by private citizens, Russia, Iran and other state actors also do so. This approach makes it difficult to detect, monitor and investigate attacks. The appeal of internet connected devices owned by private citizens is that these are seldom updated and therefore have greater vulnerabilities.

"When it comes to cyberattacks launched by foreign powers, several states are active but the two that carry out most attacks and present the greatest security risk to Sweden are Russia and China. The approaches used by foreign powers vary somewhat. In some cases, they use employees of their own security services to carry out attacks directly from their offices. In other cases, they use external companies or universities, to make it harder to link the attacks to the state carrying them out," explains Mia.

Foreign powers have both extensive resources and a high capability to carry out electronic attacks. Many countries have separate departments within their intelligence and security services to conduct intelligence gathering via cyberattacks. These hackers are sometimes referred to as advanced persistent threats (APTs). While only a small percentage of these actors carry out electronic attacks to destroy other states' infrastructure or critical societal functions, many have the capability to do so. ■

** This individual has been anonymised for security reasons.*



Cooperation to protect

The Swedish Security Service works purposefully and farsightedly to detect and prevent crimes that threaten national security, to counter terrorism and protect the Swedish central government.

Sweden

The Swedish Security Service in brief

The Swedish Security Service is a national security service tasked with preventing threats to Sweden's security and democracy. The Security Service conducts security and intelligence operations to protect the Swedish central government and Sweden's secrets, as well as to counter espionage, violent extremism and terrorism.

Operational areas and regional offices

Counter-intelligence

The Swedish Security Service prevents and detects espionage and other unlawful intelligence activities, whether targeting Sweden and Swedish interests abroad, foreign interests in Sweden or refugees seeking asylum in the country.

Protective security

The Swedish Security Service's work with protective security is preventive and long-term. Protective security involves raising the level of societal security through analyses, records checks, supervision and recommendations to government agencies and companies that conduct the types of activities that may have a bearing on Sweden's national security.

Counter-terrorism

The Swedish Security Service prevents and averts the commission of terrorist offences, such as attacks or incitement of terrorism, or the financing of, training in, recruitment to, or association with a terrorist organisation.

Counter-subversion

The Swedish Security Service prevents and averts crimes intended to subvert the fundamental functions of democratic government.

Dignitary protection

The Swedish Security Service is responsible for the security of members of the Swedish central government, and of foreign diplomats and dignitaries on state visits or attending similar events. Close protection is largely a matter of preventive measures to ensure that the protectee can go about their business in a safe and secure manner.

The Swedish Security Service's remit also includes counter-proliferation and aliens-related cases. Counter-proliferation involves preventing the proliferation, procurement and production of weapons of mass destruction. This work is carried out in close cooperation with other government agencies. The Security Service's work with alien cases is meant to prevent individuals who may pose a threat to national security from staying or settling in Sweden. One important part of preventive work is the agency's remit as a consultative body to the Swedish Migration Agency.

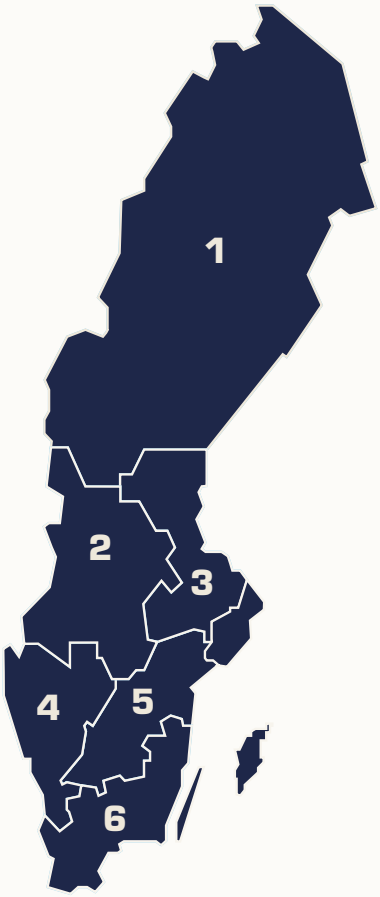
Intelligence

The Swedish Security Service conducts intelligence gathering nationally and internationally. This is part of its remit to prevent and expose crimes against Sweden's national security. In Sweden, intelligence is gathered through surveillance, sources, and discussions and contacts with other government agencies and organisations. Internationally, intelligence is mainly gathered through cooperation with other security and intelligence services. The intelligence gathered by the Swedish Security Service is processed and analysed and, in some cases, a preliminary investigation is launched or some other measure is taken. Intelligence is also sometimes shared with the Swedish Government, other government agencies or organisations to enable them to take appropriate measures within their areas of responsibility.

Governance and transparency

The Swedish Security Service reports to the Swedish Government and is headed by the Head of the Swedish Security Service. The Security Service is governed by the letter of regulation and instructions issued by the Government specifying the objectives and remit of the Security Service, as well as by various statutes such as the Swedish Police Act (SFS 1984:387). Most of the governance, planning and reporting documents related to the Swedish Security Service are classified as a matter of national security. For operational and security reasons, the Swedish Security Service is not often able to be open about what it does and why it does so.

The Swedish Security Service is subject to supervision by the Office of the Chancellor of Justice and the Parliamentary Ombudsmen (JO). The Commission on Security and Integrity Protection supervises and carries out inspections of the Security Service's processing of personal data and, at the request of an individual, checks whether they have been subject to covert intrusive measures. The Government also appoints members to the Swedish Security Service's Oversight Council, which is tasked with exercising civil oversight. All parties in the Riksdag are represented on the council.



The Swedish Security Service – a national security service

The Swedish Security Service operates nationwide. The agency has six regional offices in addition to its head office in Solna. Regional operations are conducted in all of the agency's areas of operation. The offices are located in:

1. Region North in Umeå: The counties of Jämtland, Norrbotten, Västerbotten and Västernorrland.
2. Region Bergslagen in Örebro: The counties of Dalarna, Värmland and Örebro.
3. Central Region in Uppsala: The counties of Gävleborg, Uppsala and Västmanland.
4. Region West in Gothenburg: The counties of Halland and Västra Götaland.
5. Region East in Linköping: The counties of Jönköping, Södermanland and Östergötland.
6. Region South in Malmö: The counties of Blekinge, Kalmar, Kronoberg and Skåne.
Head office: Solna The Swedish Security Service's Head Office covers the counties of Stokholm and Gotland.

Work intensifies to deal with threats to Sweden

The significantly deteriorated international situation has not only affected Sweden's security but has also had an impact on the Swedish Security Service and its activities.

"As the international situation has changed, we note that Russia has an increasing need to gather intelligence. At the same time, China and Iran continue to present a serious security threat to Sweden. As a result, we as an agency have ramped up our counter-espionage work," says Magnus Krumlinde, Deputy Head of the Swedish Security Service.

This increased focus on counter-espionage work involves the Swedish Security Service intensifying its work to decrease the ability of foreign powers to act as well as strengthening the resilience of critical activities. This is achieved both by impeding and preventing the unlawful intelligence operations of foreign powers and by raising awareness of the threats foreign powers pose.

"We have been strengthening our national and international cooperation for several years, which is important in the global world we live in. Following the invasion of Ukraine, we have further intensified such cooperation, a necessity if we are to protect Sweden together with others," says Magnus Krumlinde.

Russia regards Sweden as part of the collective West, which supports Ukraine in many different ways. In view of this, Russia is keen to understand other countries' reasoning and what decisions that are likely to make, including about NATO. The risk of cyberattacks has also increased.

"We must cope with the broad and accelerating threat from foreign powers, and the changing international situation will affect the course of our work for a long time to come. An eventual NATO membership would make the Swedish Security Service part of a new context," says Magnus Krumlinde.

"At the same time, the work involved in our remit as a whole continues. That is to say, dignitary protection, protective security, counter-terrorism and, not least, our counter-subversion remit at a time when we note anti-state tendencies, subversive activities and an increasing mistrust of society," says Magnus Krumlinde. ■

> *We must cope with the broad and accelerating threat from foreign powers, and the changing international situation will affect the course of our work for a long time to come.*
>
> *Magnus Krumlinde, Deputy Head of the Swedish Security Service*

Production: Swedish Security Service
Graphic design: Intellecta
Illustrations: Fredrik Tjernström
Photo: Swedish Security Service, TT
Printed by: Stibo Complete A/S Horsens Denmark

ISBN: 978-91-86661-24-3
How to order: The publication can be downloaded from www.sakerhetspolisen.se or ordered via: sakerhetspolisen@sakerhetspolisen.se

The Swedish Security Service is responsible for ensuring that what must not happen does not happen. Therefore, our work is preventive. We avert threats to Sweden's security and to our citizens' rights and freedoms. Because our mission is to secure the future of our democracy. This we carry out resolutely and with a long term perspective. We protect the central government and Sweden's secrets. We counter espionage, extremism and terrorism. For us, the most important incidents are the ones that never happen.

Säkerhetspolisen
Swedish Security Service