The Swedish
Security Service

2025
–
2026

CONTENTS

Charlotte von Essen, Head of the Swedish Security Service.

The Swedish Security Service – steadfast in uncertain times

Sweden is experiencing turbulent and uncertain times, with difficult-to-assess threats and rapid changes. In a time when the world order is being challenged and disrupted, the security of Sweden is affected. Working together with partners and allies strengthens Sweden's security, enabling us to anticipate the unpredictable and take timely action.

For several years, the security situation in Sweden has been serious. The security situation is affected to a great extent by what is happening in the world, and the past year has continued to be characterised by rapid changes coupled with considerable uncertainty about future developments. During the year, incidents have occurred to indicate that the long-standing, rule-based world order is being challenged and disrupted. The same applies to established forms of cooperation. These changes could be exploited by hostile foreign powers to create discord and division.

Amid these rapid developments, it can be difficult to predict threats and their consequences. Our cooperation with national and international like-minded partners has been intensified in order to obtain the best possible view of the situation, thereby helping us to enhance Sweden's security.

Negative trends

The threat to Sweden is assessed to continue to develop in a negative direction over the next few years. This threat is mainly affected by Russia's objectives and Russia's security-threatening activities in the vicinity of Sweden and where Russia remains the greatest threat to Sweden.

The main activities carried out by the Russian intelligence and security services are intelligence activities, influence operations, and technology procurement. There is also a threat of Russian sabotage targeting Western support for Ukraine. In our assessment, Russian security-threatening activities could increase. We have found that Russia is more inclined to take greater risks than before. This development is characterised by more offensive action, with covert influence activities being carried out against European countries, including Sweden.

Russia has a persistent need to procure know-how, technology, and products in order to strengthen its capability, and it repeatedly attempts to circumvent the imposed sanctions. In order to strengthen Europe's – and thereby also Sweden's – security, we all need to do more to make it more difficult, costly, and complicated for Russia to continue waging war.

China and Iran, with their intelligence and security services, also pose a significant threat. China remains the long-term threat in terms of Sweden's financial

security. China's objective is to have long-term control over and dominate key areas such as world trade and economics. This could also be a matter of creating dependencies that could be used for influencing purposes.

Sweden has, of course, a great need to cooperate with other countries in areas such as research, innovation, and trade. However, as Head of the Swedish Security Service, I would also like to emphasise that there are some areas in which it is not prudent to cooperate with certain countries, as this may risk jeopardising significant critical assets and Sweden's security. This ultimately concerns Sweden's sovereignty and prosperity. In the current situation, where relations between countries are being challenged and changing, it is also important that previous dependencies are not replaced by new ones.

Iran has, for a long time, engaged in security-threatening activities against Sweden, by e.g., gathering intelligence and compiling information about dissidents, and has also carried out acts of violence. It remains to be seen how recent developments in Iran will affect the future threat posed by Iran.

There are several states which, on their own or together with other states, conduct security-threatening activities against Sweden. When these countries collaborate, this makes the threat more complex, which could increase the threat to Sweden. To be prepared for such a development, we have expanded our resources and capabilities so that we can continue to work sustainably, persistently, and methodically.

The hybrid threat

As a national security service, we are tasked with preventing, detecting, and responding to threats and vulnerabilities that affect Sweden's security. Our Service's intelligence, along with information obtained from others, is essential, not only because it enables us to follow developments and to detect any escalation of the situation, but also because it enables us to take timely action.

In recent years, many incidents and aberrations, such as cable damage, drone overflights, and cyberattacks, have been reported to the Swedish Police Authority. Our Service's role in this context is to analyse and assess if a foreign power could be behind a particular incident, or if it was a matter of e.g. sabotage carried out with the aim of having a detrimental effect on Sweden's security and, if so, to assume responsibility for handling this. Great steps forward have been taken together with other authorities in order to increase incident-related coordination, so that those affected can take decisive action when required.

Thus far, Sweden has not been subject to extensive attack attempts or traditional sabotage. However, we have noted a number of cases of attempted cyber sabotage by Russia, and we know that the intelligence threat is high. It is evident that the intelligence and security services of hostile foreign powers continue to carry out extensive security-threatening activities against Sweden.

In the current security situation that is fraught with uncertainty, it is important that affected actors continue to be vigilant and ready to act when necessary. However, it is also important to refrain from drawing hasty conclusions when something has happened, as this entails a risk of playing into the hands of hostile foreign powers, using resources in the wrong way and, in the worst case, causing the situation to escalate further.

»There are several states which, on their own or together with other states, conduct security-threatening activities against Sweden. When these countries collaborate, this makes the threat more complex, which could increase the threat to Sweden. To be prepared for such a development, we have expanded our resources and capabilities so that we can continue to work sustainably, persistently, and methodically.«

Protecting critical assets

Due to the negative developments around the world, Sweden's resilience needs to increase. The necessary work is currently underway to expand Sweden's military as well as civil defence capabilities. In these efforts, protective security is an important element.

Many organisations that are of significance to total defence are in a growth phase in terms of staffing. As organisations grow, it is important that their security-related work increases as well, especially the work concerning personnel security. An insider in an

organisation could cause great harm. We, the Swedish Security Service, therefore need to take decisive action whenever there are suspicions of such seriously harmful activities.

Elevated terrorist threat level

Besides the threat from hostile foreign powers, we need to handle the terrorist threat. The terrorist threat level in Sweden remains elevated. This entails that a terrorist attack could occur, meaning that, in spite of lowering the terrorist threat level last year, we cannot sit back and relax. The threat stems mainly from violent Islamism and violent right-wing extremism. The threat of attack is mainly associated with lone actors or small groups acting against easily accessible targets using relatively simple means.

We have also noted a trend in which violence itself may be a stronger driving force than ideological motives. Individuals are increasingly shifting between different groups and contexts that advocate the use of violence, and are composing their own ideologies based on the contexts they find themselves in. I find it very concerning that our intelligence information indicates that so many young individuals are being drawn to extreme violence.

A number of changes have been made to Swedish legislation in recent years, and this has given us better tools to prevent terrorist crime. This has had an impact, and several of our operations in the past year have led to trials and convictions for e.g., terrorist offences, preparation to commit a terrorist offence, participation in a terrorist organisation, financing of terrorism, and terrorist travel.

However, we are facing challenges in detecting threat actors in the digital environment. We have a growing requirement for a revised regulatory framework that gives us the flexibility we need to quickly collect, process, and store information. Due to the serious security situation and the very uncertain situation in the world, we must enhance our capability to detect new threats and phenomena that could affect Sweden's security. Information processing is an absolutely crucial part of this.

A secure general election in Sweden

In September of this year, a general election will be held in Sweden. The election is taking place at a time when the security situation is serious.

We know that Sweden is subject to security-threatening activities and malign influence attempts from foreign powers, especially from Russia. The fact that a general election will take place could possibly be exploited by hostile foreign powers, which could use influence campaigns to attempt to fuel conflicts in Sweden and to influence the credibility of and confidence in the election. Along with other relevant authorities, we are closely monitoring how this situation may develop, but we also must be careful about drawing hasty conclusions about suspected election interference. Hostile foreign powers are not behind everything that occurs.

In addition, we assess that Sweden's resilience against election interference is excellent. The election process, with its robust electoral system, is difficult to manipulate. Also, the public in Sweden is generally suspicious of and not very receptive to Russian influence and propaganda. There is general political consensus about support for Ukraine and the investments being made in the defence sector, which further increases our resilience.

Strengthening the intelligence system

The structure of the Swedish intelligence community is changing. A new authority will be established – a civilian foreign intelligence service. As a national security service, the Swedish Security Service will still be responsible for assessing what may affect Sweden's domestic security. As a whole, these changes reflect higher aspirations in terms of intelligence-related work.

In the enquiry report upon which these changes were based, it was assessed that there was a need to change the legislation to give the Swedish Security Service what it requires in order to be an effective organisation. We welcome the proposal because, in our view, such a change is a necessary development, enabling the Security Service to cope with the deteriorated security situation.

Consistently stable

Developments in Sweden and across the world show just how complex and difficult it is to assess the threats, and how they increasingly overlap and intertwine. The only predictable thing is the unpredictability of the situation.

In the turbulent security situation, when Swedish security and key democratic values are being challenged, the work of the Swedish Security Service is more important than ever. This means that we, together with our partners and allies, need to act in unison and remain steadfast in a world that is anything but stable.

The Swedish Security Service remains steadfast in these uncertain and changing times in its duty to protect Sweden. ■

Magnus Krumlinde, Deputy Head of the Swedish Security Service.

The Russian threat is mitigated through resistance

We are in the midst of an unsettled international situation that also affects Sweden and Sweden's national security. Cyberattacks, malign influence attempts, and threats to dissidents are a few examples of hybrid security-threatening activities carried out by hostile foreign powers. We have also noted cases of sabotage, murder, and planned terrorist attacks in NATO countries that have been carried out by the security and intelligence services of foreign powers. One country stands out in terms of both the security and the intelligence threat: Russia.

Russia has waged a war of attack and attrition against Ukraine for over four years. Russian attacks are carried out on a daily basis against energy facilities, people's homes, industries, and authorities. Thousands of civilian Ukrainians have been killed, Ukrainian children have been kidnapped, and entire cities have been bombed to pieces by Russia. However, Ukraine has demonstrated a resilience and determination to defend itself that has surprised many and inspired everyone.

Since Russia's full-scale invasion of Ukraine in February 2022, Sweden has contributed by providing extensive military, humanitarian, and civil/civilian support to Ukraine. The Swedish Security Service has also been involved by helping to counter and limit Russian military capabilities in Ukraine and assisting in reinforcing Ukraine's defence. In addition, the Swedish Security Service is responsible for ensuring the safety of members of the Central Government during their trips to Ukraine, which several of them have taken.

Although the support from Sweden and the Nordic countries to Ukraine is important, more needs to be done to make it more difficult, costly, and complicated for Russia to continue waging war. The amount of financial support that Ukraine receives from the EU is lower than the amount of money that Russia makes through its sales of oil and gas. In spite of this, the EU has curtailed Russia's scope of action and capabilities several times by imposing various sanctions.

Although sanctions against Russia have been in place since Russia's unlawful annexation of Crimea in 2014, they have been expanded since then. The sanctions currently include everything from a wide range of export and import bans to economic sanctions targeting Russian individuals and companies, as well as specific sanctions that target various sectors of Russian society, business and trade. The sanctions also include a requirement for companies in the EU to make every reasonable effort to ensure that they do not help other countries to export sanctioned goods to Russia.

The Swedish Security Service is one of the authorities working to ensure that the EU trade sanctions are upheld. Sanctions legislation in Sweden has recently been expanded and tightened, primarily by introducing broader criminalisation provisions and stricter penalties. If someone in a company violates a sanction, it falls upon the Swedish Police Authority or the Swedish Security Service to investigate the matter in cooperation with other authorities. The individual could face a significant penalty. In addition, the company itself could be fined. Swedish companies that have not taken the necessary precautions to counter the risks of their products becoming available to Russia may also be held partly responsible for the suffering that is taking place in Ukraine.

> A key insight is that security and resilience are strengthened through cooperation and collaboration.»

Ukraine's resilience is a source of inspiration for building a strong Sweden. As total defence is being expanded and more Swedes are becoming involved, it is important to learn from the experiences of countries that are currently at war. A key insight is that security and resilience are strengthened through cooperation and collaboration. This involves safeguarding Sweden's security through robust protective security measures as well as keeping abreast of the threats against Sweden.

Sweden's security continues to be challenged by the unsettled international situation, with Russia clearly posing the greatest threat. Therefore, supporting Ukraine and making it more difficult for Russia to wage its unlawful war is not just a question of the future of Ukraine, but also of the future of Europe, the Nordic countries, and Sweden. ■

The threat to Sweden is constantly changing

Unexpected incidents and conflicts around the world have had an effect on the threat to Sweden over the past year. There are many indications that the next few years will also be marked by considerable uncertainty. This places demands on the Swedish Security Service to act both resolutely and reflectively.

Carolina Björnsdotter Paasikivi, Head of the Security Department, the Swedish Security Service.

Fredrik Hallström, Head of Operations, the Swedish Security Service.

As a national security service, we work 24/7, 365 days a year, to gain an understanding of what the threat to Sweden looks like today and what it will look like tomorrow. This knowledge forms the basis of our efforts to make Sweden a less attractive target for those wishing us harm," says Carolina Björnsdotter Paasikivi, Head of the Security Department at the Swedish Security Service.

The global situation and the threat

The threat to Sweden is subject to change and largely relates to what happens outside the country's borders. In 2025 and early 2026, various developments around the world have had both a direct and an indirect impact on the threat to Sweden, and thus also the Swedish Security Service's remit.

"For the first time in a long time, the rule-based world order is being challenged. Countries with ambitions to be global superpowers are expressing an intent to divide the world between them into various spheres of interest. As a member of the EU and NATO, Sweden's security is affected by such rhetoric and actions. Add to that the recent developments in Iran and the Middle East," says Fredrik Hallström, Head of Operations at the Swedish Security Service.

»For the first time in a long time, the rule-based world order is being challenged.«

Hostile foreign powers and violent extremists are opportunistic, in the sense that they take advantage of any given chance to further their own interest. For violent extremists, this can be taking advantage of wars and conflicts in other parts of the world to mobilise sympathisers in Sweden, while hostile foreign powers may attempt to fuel conflicts within or between countries.

"If a foreign power perceives tensions in a relationship, they can exploit this to further their own positions in a relatively simple way. There is a growing risk that hostile foreign powers will attempt to test our resilience. This is especially the case with Russia," says Fredrik Hallström.

To a considerable degree, the threat to Sweden is affected by events around the world that are outside our control. Expanding and enhancing Sweden's protection, however, is something that we can control.

"What we as a country can actually control independently is the protection of our critical assets, regardless of threat levels. There are several areas in which protection must be improved. For example, hostile foreign powers are interested in cutting-edge Swedish research. Technology that can be used within the total defence is also of interest to foreign powers. For this reason, it is vital that we have strong protection in these areas," says Carolina Björnsdotter Paasikivi.

The hybrid threat

In addition to security-threatening activities such as espionage and unlawful procurement of technology, there are several recent examples where hostile foreign powers have used other methods against targets in Europe. These include cyberattacks, sabotage, and influencing attempts.

These types of hybrid activities are often carried out by proxy to reduce the risk of detection.

"Security-threatening activities carried out by foreign powers always fall under the remit of the Swedish Security Service, regardless of the method used. Our Service has the knowledge to determine whether a foreign intelligence or security service is behind an incident," says Fredrik Hallström.

Over the past few years, there has been speculation that a number of incidents in Sweden, involving for example mobile phone towers and water facilities, were the result of sabotage or involvement by foreign powers. In several of these cases, the Swedish Security Service's investigations showed that no foreign powers were involved, and that these incidents were instead accidental or cases of wilful damage carried out by lone actors with no links to foreign powers.

"There is a substantial risk that hostile foreign powers may engage in sabotage targeting Sweden in the future. At the same time, it is important to avoid drawing conclusions before we have properly established what actually happened and who is behind the incident. Serious incidents do occur, but not always at the hand of foreign powers. Falsely attributing activities to foreign powers helps them obtain their objectives without them having to actually do anything," says Fredrik Hallström.

One aim of foreign malign influence directed at Sweden is to increase polarisation, spread fear among the public, and amplify a narrative that is in line with the foreign power's own long-term interests. Often, this involves ensuring the survival of the regime and its position of power.

"Russia wants to spread an image of a Europe that is falling apart and undermine our support for Ukraine. By critically evaluating the sources of information, and considering who might benefit from the dissemination of such information, we can all contribute to protection against malign influencing attempts," says Carolina Björnsdotter Paasikivi.

Blurred boundaries

As a result of how foreign malign influence has developed and changed, the Swedish Security Service's counter-terrorism and counter-intelligence efforts have grown closer. The boundaries between terrorism, foreign malign influence, and other criminal activities are becoming blurred.

Foreign powers use criminals as proxies to carry out activities, and to a greater extent than before, the targets of terrorist activities coincide with the targets of foreign powers. New technology, not least related to the use of AI, also strengthen the capabilities of those wishing to harm Sweden.

"The new threat landscape is very obvious when viewed through the Swedish Security Service's lens. We are working in completely new ways. The traditional divisions between our various operational areas are disappearing. Cross-expertise cooperation, such as between police officers, IT specialists, and psychologists, is becoming more important. As the world changes, so must we. This is how we counter the threat, build up protection, and keep Sweden safe," says Carolina Björnsdotter Paasikivi.

»We always do our utmost to reduce threats to Sweden before they are put into practice.»

The overall assessment of the terrorist threat to Sweden is that violent Islamism and violent right-wing extremism remain the greatest threats. The most probable perpetrators are individuals who have been radicalised through propaganda that glorifies violence, and who act alone.

The Swedish Security Service has several tools at its disposal to reduce the threat to Sweden. This includes everything from cooperating with other government authorities to make it difficult for those who wish us harm to operate in our country, to initiating criminal investigations with the aim to pursue legal action.

"We always act as early as possible to reduce threats. We cannot afford to be passive. One of the tools at our disposal is the initiation of a criminal investigation. Our definition of success is not always a conviction, but rather acting early and reducing a potential threat. We always do our utmost to reduce threats to Sweden before they are put into practice," says Fredrik Hallström. ■

This assessment in brief

Hybrid activities

Several countries are engaged in malign influence against Sweden and Europe in general, but Russia stands out in this regard. Some of Russia's security-threatening activities against the West also include hybrid actions that aim to create concern, to polarise, and to mislead. The purpose could also be to test the West's reactions and preparedness.
➔ *Read more on pages 14–17.*

Russia, China, and Iran

While Russia, China, and Iran pose the most significant threats to Sweden, there are other states that also engage in security-threatening activities. These states increasingly collaborate and reinforce one another, which has resulted in a greater threat to the West, including Sweden.
➔ *Read more on pages 18–21.*

Unlawful technology procurement

Swedish technology and know-how continue to be highly prioritised by the security and intelligence services of hostile foreign powers, with these being used in the war against Ukraine, or for other kinds of security-threatening activities. Russia uses an advanced state-controlled system to access Western products, technology and know-how in order to circumvent sanctions and maintain its military capability.
➔ *Read more on pages 22–25.*

Personnel security – a vital part in protecting Sweden's security

With the expansion of the Swedish total defence, more and more people are involved in security-sensitive activities. Security screening of personnel is an important tool for preventing sensitive information or other critical assets from ending up in the wrong hands.
➔ *Read more on pages 26–33.*

Subversive threats

The most severe subversive threat to Sweden is assessed to be associated with organisations and networks that covertly carry out their activities to achieve long-term goals. The motives could be ideological, personal, or financial. The Swedish Security Service's current assessment is that while there are actors who have the intent to carry out subversive activities, they do not have the capability to pose a concrete and severe threat.
➔ *Read more on pages 34–35.*

Cyberattacks

Cyberattacks targeting both private and public entities take place all the time. Due to developments in technology, the methods used to carry out these attacks are constantly changing and becoming increasingly accessible. An attacker may be a hostile foreign power or some other type of actor, such as criminal groups motivated by financial gain.
➔ *Read more on pages 36–39.*

The threat of attack associated with violent extremism

The terrorist threat to Sweden is mainly associated with lone actors or small groups that act against accessible targets using relatively simple means. The threat stems primarily from violent Islamism and violent right-wing extremism. However, there are also indications that violence itself may be a powerful driving force.
➔ *Read more on pages 40–43.*

Decreased scope of action for violent extremism

The Swedish Security Service's intelligence efforts aim to detect, prevent, and counter threats. In order to decrease the scope of action for violent extremism, it is necessary to systematically reduce the platforms used for recruitment and radicalisation. By working together with other authorities, the Swedish Security Service has decreased the scope of action for violent extremism in Sweden in recent years.
➔ *Read more on pages 44–47.*

Working together to secure the general election

Cooperation between authorities is key to ensuring that a general election can be held securely. As a national security service, it is the Swedish Security Service's remit to detect, prevent, and counter crimes against Sweden's security. Sweden has a robust electoral system with a transparent election process that is difficult to manipulate. However, there are hostile actors who may have an interest in weakening the Swedish democratic system.
➔ *Read more on pages 48–49.*

Malign influence from foreign powers

Foreign powers employ a number of methods in their malign influence attempts against Sweden and Europe in general. The Swedish Security Service conducts extensive intelligence efforts and takes various measures in order to limit the scope of foreign powers' malign influence attempts in Sweden.

Malign influence against Sweden is carried out in a number of different ways. This could be a matter of political schemes, threats, or provocation. It could also involve carrying out economic influence by threatening or exerting pressure on companies and businesspeople. Sabotage and information influence are other activities that could be employed against society for malign influence purposes. Malign influence can be carried out overtly, covertly, or in a plausibly deniable manner.

While several countries are engaged in malign influence against Sweden and Europe in general, Russia stands out in this regard. Some of Russia's security-threatening activities against the West consist of malign influence activities meant to create concern, to polarise, and to mislead. The purpose could also be to test the West's reactions and preparedness.

"This year, the Swedish Security Service has conducted extensive intelligence work and analysed events and incidents in order to create an assessment of the situation that is as complete as possible," says Ali*, an Analyst at the Swedish Security Service.

Information influence

Russia has long engaged in information influence against Sweden and Europe in general. This type of activity continues to be prioritised by the Russian regime. This is not infrequently a matter of narratives that portray certain countries as hostile to Russia, or rhetoric that reinforces polarising issues in a society. These activities are based on Russia's security-related political aims, which are to ensure the survival of its own regime, weaken NATO cooperation, and undermine Western support to Ukraine.

"The possibility for Russia to successfully carry out influence campaigns is limited by the strong support for Ukraine in Sweden, the broad political consensus concerning the resistance to Russia, and the low degree of receptiveness that the Swedish population has to pro-Russian ideas. However, it is necessary to be

vigilant in regards to influence attempts. It is important to evaluate information sources and to have a critical mindset about information," says Ali.

As several Russian intelligence officers working under diplomatic cover have been expelled from Sweden, Russia has needed to use other platforms from which to run its intelligence and influence activities. This could, for example, be a matter of using intelligence officers who temporarily travel to Sweden, or of using organisations in Sweden with links to the Russian state.

An example of such a platform is the Russian-Orthodox Church of the Moscow Patriarchate. The Swedish Security Service has, for several years, noted that the Russian state uses this Church as a platform in order to engage in intelligence gathering as well as other security-threatening activities consisting of malign influence attempts against Sweden and individuals in the Russian diaspora in Sweden. The Swedish Security Service has taken measures, in cooperation with other authorities, to reduce the possibility for Russia to use this Church as a platform to carry out security-threatening activities.

The hybrid threat

There is a concrete threat of sabotage from Russia. Sabotage is part of the Russian strategy to destabilise countries in Europe. Particular priority is given to targets that affect the West's possibilities of supporting Ukraine.

There are several cases in which Russia has carried out such activity against European countries. For example, Russian drones violated Polish airspace in September 2025, which led Poland to invoke NATO Article 4, under which NATO members may seek consultation with other NATO members in connection with a security threat.

In the past year, there have been reports in Sweden of damage to mobile phone towers, undersea cable damage in the Baltic Sea, and other cases of suspected sabotage.

"The Swedish Security Service has, in the past year, assessed cases of suspected sabotage against, for example, undersea cables, power stations, and water facilities. It has thus far not been possible to attribute any of the cases of physical sabotage to foreign powers," says Ali.

There are, however, incidents where the Swedish Security Service has been able to confirm that foreign powers have been involved. In the past year, for example, cyberattacks have been carried out that are linked to Russian intelligence and security services.

"It is important to take action when this is warranted but, at the same time, avoid drawing hasty conclusions and assuming that Russia is behind each and every incident, as this could create unnecessary alarm, cause the situation to escalate, and result in the misallocation of public resources. This is exactly what hostile foreign powers hope to achieve. However, we must not be naive, but be prepared for the possibility that sabotage by a foreign power could occur," says Ali.

In the aftermath of incidents and other developments, the Swedish Security Service has noted a clear tendency towards an increase in the reporting of similar developments and a heightened awareness of these.

»Sweden needs to build up a capability that enables society as a whole to cope with the complex threat posed by hostile foreign powers.»

"It is great that the public is vigilant when they observe out-of-the-ordinary things, and report what they see. There could, however, be difficulties associated with this. For example, it is very difficult to determine with the naked eye whether something flying around in the sky is a drone or something else, especially in the dark," says Ali.

Cooperation to enhance capability

The Swedish Security Service has enhanced its cooperation with several other Swedish authorities since Russia attacked Ukraine in 2022. One of the results of this increased cooperation is that other authorities are receiving more information about the threat posed by Russia. The goal is for Swedish authorities to obtain a better overall picture of the situation and a shared understanding of what this threat actually entails.

"Sweden needs to build up a capability that enables society as a whole to cope with the complex threat posed by hostile foreign powers, where every sector in society has to work towards the same goals. This capability has now been considerably strengthened," says Ali. ■

** Ali is a fictitious name.*

Russia, China, and Iran

Sweden is subject to extensive security-threatening activities carried out by hostile foreign powers. While Russia, China, and Iran pose the greatest threats to Sweden, there are additional countries that also engage in security-threatening activities. This includes intelligence activities, covert and plausibly deniable influence activities, and cyberattacks.

There is a notable trend where several states whose activities pose a threat to Sweden, and the West in general, are cooperating with and amplifying one another to a greater extent than ever before. This results in an increased threat, and the Swedish Security Service has strengthened its resources and capabilities to better be able to counter it.

Russia

Russia remains the greatest threat to Sweden. Russia mainly engages in intelligence activities, malign influence operations, and technology procurement. There is also a Russian sabotage threat that mainly targets the West's support for Ukraine. Since invading Ukraine, Russia has been taking more risks and acting more opportunistically outside the conflict area. While becoming a member of NATO has strengthened Sweden's security, it has also increased Russia's intelligence interest in Sweden.

Intelligence activities

Russia conducts intelligence activities targeting Sweden. Russia's intelligence gathering focuses mainly on information that concerns Swedish political stances, Swedish efforts with regard to NATO, and the Swedish military equipment industry. There is particular interest in Swedish support for Ukraine. Information is also gathered for more long-term war preparatory reasons, both in terms of military capabilities and critical infrastructure.

Russia is very interested in tracking and monitoring the Russian diaspora in Sweden. One reason is to exploit Russian citizens domiciled in Sweden for intelligence-gathering purposes. Another is to monitor the activities that opponents of the Russian regime carry out in Sweden, with a view to controlling the image of Russia that is being spread. The Swedish Security Service has also seen instances in which critics of the Russian regime in Sweden have had threats of attacks directed against them.

Malign influence and sabotage

When it comes to malign influence attempts, the focus of the Russian intelligence and security services is to decrease Western support for Ukraine and reinforce polarisation in order to weaken the West. Russia has conducted influence campaigns in Europe, linked to, for example, democratic elections in other countries and polarising issues such as immigration policies.

Furthermore, Russia engages in hybrid activities such as influence operations and acts of sabotage targeting Europe. These activities are becoming more and more offensive. Several European countries have pinpointed Russia as being behind influence operations and acts of sabotage in 2025. Currently, Sweden is not the primary target of these types of activities.

During the past few years, Russia has carried out more and more acts of sabotage in Europe. One method used for these activities is the use of disposable agents. These are individuals who are recruited, often in a digital environment, to carry out single missions. Russia has no interest in what happens to these individuals once their missions have been completed. These agents lack the capability to carry out more complex tasks, and are often unreliable, with money being a common driving force. The use of disposable agents allows for a higher degree of plausible deniability in the involvement of sabotage conducted by Russia.

Technology procurement

Russia has an extensive need to procure technology and know-how, within the civilian and military sectors alike, not least in order to support its warfare in Ukraine. The sanctions against Russia aim to prevent this. The Russian intelligence and security services play an important role in the attempts to unlawfully procure technology. Business arrangements that use other countries, such as China and Iran, as intermediaries are used to circumvent sanctions. ■

China

When it comes to Sweden's financial security, China still poses the long-term threat. China's ambition is to exert long-term control and dominance over key issues such as world trade and economy. The Chinese state uses resources throughout its entire society, through lawful and unlawful methods alike, to obtain their security-policy objectives. The goals of China's security-threatening activities are to obtain stability for the Chinese communist party's regime, technological dominance, financial control, and an enhanced military capability.

The Chinese intelligence and security services predominantly target financial associations and Swedish technological expertise. The goal is to strengthen China's own domestic capabilities. Another aim is to create dependencies that may be used for influence purposes.

Chinese intelligence and security services have an interest in monitoring and influencing Chinese dissidents and minority groups in Sweden. Chinese citizens are also put to use for intelligence gathering purposes.

The Chinese intelligence and security services are very capable of carrying out cyberattacks for the purpose of procuring sought-after know-how and technology. This is a modus operandi that is used to get access to information on political decision-making, as well as technological expertise, in the targeted countries.

It is in China's interest to use both lawful and unlawful methods to procure Swedish technology and know-how, with the aim to increase its own technological, financial, and military capability. As such, China has a particular interest in critical activities carried out at Swedish companies and universities and by researchers and other experts. One way to gain access to information and create dependencies is through various types of investments. Several different methods are used to circumvent legislation that places limitations on such investments, including the use of front companies. ■

Iran

In late February 2026, the US and Israel initiated a military operation against Iran. Iran's supreme leader and several other high-ranking officials of the regime were killed in the first few days of the war.

For many years now, the Swedish Security Service has described how Iranian intelligence and security services conduct security-threatening activities in and against Sweden.

Considering the recent developments in Iran, it is not currently possible to assess what threat the country will come to pose going forward – it will all come down to Iran's future regime.

The security-threatening activities that Iran has engaged in include threats, exerting pressure, and monitoring Iranian dissidents in Sweden. Iran also attempts to circumvent sanctions to gain access to Swedish technology and research, not least relating to the country's nuclear weapons program. Iran has used criminal networks as proxies to carry out acts of violence directed at Israeli and Jewish targets in Sweden.

The Israeli and US military operation against Iran, and Iran's retaliatory measures, have led to an increase in the threat to US, Israeli, and Jewish targets in Sweden. ■

Extensive unlawful technology procurement

by hostile foreign powers

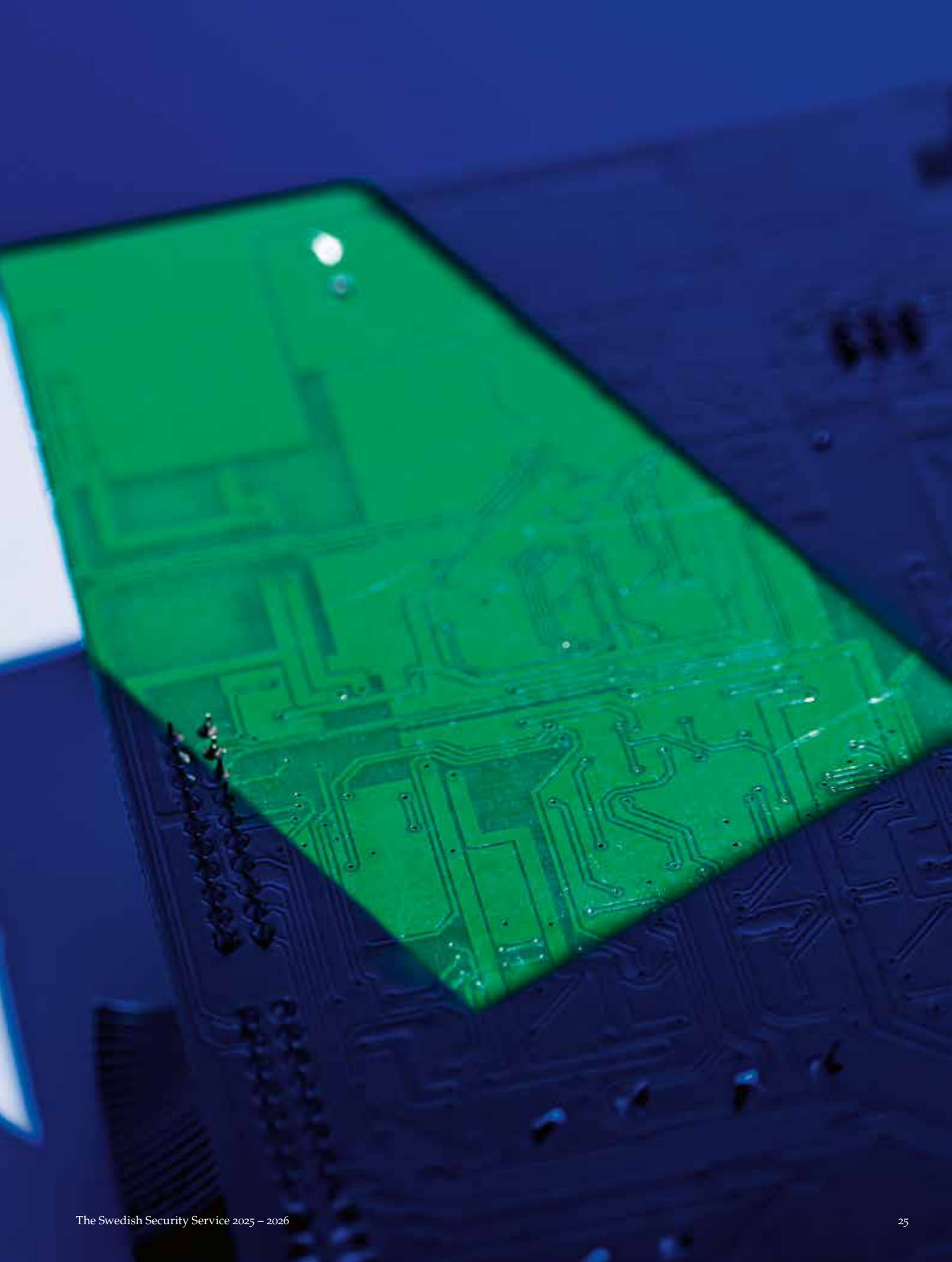
Swedish technology and know-how continue to be highly prioritised by the security and intelligence services of hostile foreign powers, for use in the war against Ukraine or for other kinds of security-threatening activities. Violations of sanctions legislation may be highly punishable, where punishment may be imposed regardless of whether or not there was an awareness that the products would eventually end up with the Russian military.

Swedish universities, research institutes and companies are at the cutting edge of innovative, emerging, and strategic technologies, and Swedish industry is a successful competitor in the global market. Hostile foreign powers are very interested in stealing, buying, or in some other way procuring Swedish products, technology and know-how.

As a consequence of the war in Ukraine, Russia is the country subjected to the most sanctions. The Russian military power has, for many years, been outdated and urgently requires spare parts, and the need for products and technology from the West has increased considerably due to the war against Ukraine. In order to circumvent sanctions, and in an attempt to sustain its military capabilities, Russia uses an advanced state-controlles system to access Western products, technology, and know-how.

The Russian procurement system has been highly prioritised politically, and resources have been allocated accordingly. Russian intelligence and security services play an active role in this system, and it is not seldom that they are both client and contractor in the procurement system. The driving forces behind this advanced, extensive procurement system will remain in place for as long as the war in Ukraine continues, and as long as the sanctions against Russia persist.

As an example, in 2022 the Swedish Security Service helped shut down a Russian procurement network involving a businessman in the Stockholm area, and this individual was investigated and prosecuted for unlawful intelligence activities against Sweden and the United States. However, the Svea Court of Appeal acquitted the businessman in November 2025, as information on the technical conditions of the various products procured on behalf of the Russian military intelligence service GRU was not considered as having resulted in significant detriment to the national security of either Sweden or the US. Simultaneously, the Court of Appeal made it clear that the businessman was an intermediary in the Russian state system for product and technology procurement from the West, as he, according to the judgment, "made purchases and organised the transport of various products. It was obvious that his goal was to act in a way that would benefit Russia".



Stricter requirements for Swedish companies

As Russia is using Western products in the war against Ukraine, the EU decided to issue strong sanctions in an attempt to prevent this from occurring. While these sanctions may not be able to stop all deliveries from reaching Russia, they still play an essential role in making the delivery of such products more delayed, more expensive, and generally more difficult. The Swedish Security Service, along with the other authorities in the Swedish Sanctions Compliance Council, have been granted more extensive possibilities to prevent, investigate, and take legal proceedings against suspected sanctions violations. Stricter prison sentences, and an extension of the criminalising conditions, for example in relation to responsibility for complicity, are some of the more severe conditions imposed.

This legislation places increased demands on both the Swedish Security Service, and other law enforcement authorities.

Examples of how Russia circumvents EU trade sanctions are as follows:

Procurement networks in Sweden and in other Western countries, consisting of Russia-linked specialists who use false names and incorrect end-user certificates to purchase goods from Swedish manufacturers and import goods to Sweden from other countries. These goods are then exported through various routes to Russia.

Swedish companies' international operations are being exploited by Russian buyers who, either themselves or through middlemen, place orders with foreign subsidiaries of multinational industrial corporations that are based in Sweden. The Swedish companies' goods are then exported to the subsidiaries located abroad, which, in turn, export these goods directly or indirectly to Russia. The latter may occur without any violations of the law in the country where the subsidiary is registered.

Swedish companies' distributors, and retailers located in third countries, which have not imposed trade sanctions corresponding to those in the EU, are being used to circumvent the sanctions. Swedish companies may export goods to such foreign customers without actually being aware that these customers are ultimately reselling these goods to Russian end users through one or more stages. This reselling by foreign customers would normally have been regarded as a breach of contract, but due to a lack of jurisdiction, it is neither a violation of Swedish law, nor a violation of the EU sanctions regulations.

The Swedish Security Service is aware that Russia uses products and technology from Sweden in the war against Ukraine. Regardless of whether it is possible to trace an identified product to a specific sale made by a Swedish company or not, these companies run the risk of committing additional breaches of various provisions in the EU sanctions regulations. There could, for example, be insufficient monitoring and checks of customers and subsidiaries, lax requirements for distributors and resellers, or insufficient knowledge about, and documentation of, the risks of sanctions circumvention in third countries.

The Swedish Security Service has investigated a number of cases in which Sweden was used as a

platform to procure products, for example cases where businesspeople in Sweden were suspected of starting companies in third countries in order to, via these companies, pass technology on to Russia.

Wide-ranging procurement by Russia, China, and Iran

The interest in procuring technology and know-how from Sweden is not just for the purpose of maintaining Russian military capabilities in Ukraine. Russia, along with China and Iran, also run wide-ranging systems to procure Western technology and know-how.

In the case of Russia, this involves both civilian and military products being procured in order to, in the long-run, enhance strategic capabilities and military programs.

The Chinese state also procures know-how and technology to reach its long-term security political goals. Particularly for China, this involves attempting to establish a global high-tech dominance which, in the next stage, may be used to enhance its military capability, as well as to create critical dependencies. These dependencies may in the long run be used to exert pressure on Sweden, politically and financially, or to influence Sweden's national security.

For twenty years now, the Iranian state has been subject to sanctions in order to limit the country's possibilities to develop and produce nuclear weapons and weapon carriers, such as robots. Also in Sweden, Iran has been actively striving for a long time to try to procure products, technology, and know-how which could be used in the development and production of such weapons. In an attempt to avoid sanctions legislation, Iran is procuring civilian products that have no nuclear end-use whatsoever on their own, but that may be used in a stage of a process to produce nuclear weapons or robots. ■

The Sanctions Compliance Council in Sweden

Headed by the Swedish Police Authority, the Council is additionally comprised of representatives from the Swedish Security Service, the Swedish Economic Crime Authority, the Swedish Financial Supervisory Authority, the Inspectorate of Strategic Products, the Swedish National Board of Trade, the Swedish Tax Agency, Swedish Customs, and the Swedish Prosecution Authority.

The Council was established in June 2024, with the aim of strengthening collaboration among these authorities in order to ascertain that effective measures are being taken to ensure compliance with sanctions.

The Swedish Security Service's efforts to counter unlawful technology procurement

In an effort to counter unlawful technology procurement and sanctions violations, the Swedish Security Service undertakes various measures to provide advice and support to Swedish companies, trade associations, universities, authorities, and businesses. Close cooperation also takes place between the Swedish Security Service and many other authorities within the Swedish Sanctions Compliance Council to counter sanctions violations.

Additionally, long-term efforts are being made by the Swedish Security Service to limit the opportunities for foreign powers to make damaging foreign direct investments (FDI), in accordance with the Screening of Foreign Direct Investments Act (2023:560). In its role as a referral body for the Inspectorate of Strategic Products (ISP), the Swedish Security Service has dealt with several such cases from different countries.

The Swedish Security Service also works closely with the Swedish Migration Agency to prevent situations in which foreign citizens that pose a security threat are used by hostile foreign powers to acquire know-how and technology.

The Swedish Act on International Sanctions

The penalty for sanctions violations is up to three years' imprisonment; however, if the offence is gross, this can be up to six years' imprisonment. Two or more repeated, less serious, sanctions violations may also collectively lead to liability for repeated sanctions violations, for which the penalty is up to six years' imprisonment.

The Act also introduces the criminal offences of attempting, aiding and abetting, and instigating sanctions violations.

The responsible authorities have an obligation to submit a report if there is a reason to suspect that sanctions violations have been committed.

Personnel security – a vital part in protecting Sweden's security

With the expansion of the Swedish total defence, more and more people are involved in security-sensitive activities. Security screening is an important tool for preventing sensitive information or other critical assets from ending up in the wrong hands.

Hostile foreign powers have an interest in recruiting individuals who work in security-sensitive sectors – activities that are of importance to Sweden's security – in order to gain access to information that benefits the interests of foreign powers.

It is important to assess an employee's suitability to participate in security-sensitive activities. An individual who, in the course of their employment or otherwise, will be participating in security-sensitive activities must therefore be subject to a security screening.

"The purpose of a security screening is to assess whether an individual is loyal to the interests covered by the Protective Security Act, and whether they are otherwise reliable from a security perspective. Personal vulnerabilities that may be relevant from a security standpoint must also be assessed," says Oskar*, who works with protective security at the Swedish Security Service.

Different roles in the security screening process

As part of the security screening process that is initiated when an individual is to be hired in a security-classified position, the operator – in this case the employer – requests a records check to be carried out by the Swedish Security Service. Should any adverse information on the employee emerge as a result of this records check, it is not up to the Swedish Security Service to decide whether this information should be disclosed or not.

"Information from a records check may only be disclosed following a decision by the Swedish Agency for Oversight of Privacy Protection in Law Enforcement. An independent committee determines whether the results of the records check should be disclosed to the operator or not," says Oskar.

It is the operator who decides whether an individual is suitable for employment and whether they successfully pass the security screening process. The Swedish Security Service's records check is one of many aspects of a process that must be taken into account for a final decision to be made.

The records check can be viewed as one way of verifying some of the circumstances that were, or should have been, disclosed at the initial stage of the process, known as the basic security screening.

An ongoing process

It is unusual to take a job for the purpose of infiltration. More commonly, an individual becomes a so-called insider during the course of their employment. Predicting ahead of time whether someone is at risk of becoming an insider is difficult, and vulnerabilities may change over time. Having adequate personal information is vital for this reason, as is the follow-up security screening procedure.

"Personal circumstances change, and for that reason, so does the risk of a person becoming an insider. Examples of personal vulnerabilities that can emerge over time include financial difficulties or workplace discontent. This may tempt the individual to exploit weaknesses in the employer's operational protection," says Oskar.

A robust security culture at a workplace could positively impact the insider threat. Through day-to-day interactions, changes in behaviour or other relevant signals can be caught early. Those who frequently interact with an individual, such as their immediate supervisor or colleagues, have a better chance of detecting atypical behaviour. If an employer is made privy to the vulnerabilities of their employees, they are better

Terms

The Agency for Oversight of Privacy Protection in Law Enforcement
The Agency for Oversight of Privacy Protection in Law Enforcement comprises three decision-making bodies. One of these is the Records Checks Delegation, which decides whether information gained from a records check should be disclosed to the operator.

Operator
The operator is the entity that carries out the security-sensitive activities. This may be a company, a government authority, or a municipality.

Security screening
The operator carries out a screening of individuals whose work will include security-sensitive activities to ensure their loyalty and reliability, and to detect their vulnerabilities.

Records check
The Swedish Security Service carries out a records check as part of the security screening process for all individuals employed in the security classes 1–3. This includes checking whether the individual in question has been suspected or convicted of any crime in Sweden.

equipped to reduce any potential threats. This may include involving the occupational health service to provide help and support.

It is also important to have processes in place to receive and handle tips on irregularities.

A changing system

In the last few years, several state commissions have been launched in the area of personnel security. Two new commissions were initiated during the autumn of 2025.

One of these commissions focuses on how non-security-sensitive sectors can be protected against individuals who are unfit for employment, for example to avoid infiltration from organised crime. At present, there is no adequate regulation in place for conducting background checks for employment in these sectors.

The other commission seeks to determine whether Sweden should adopt a person-based clearance system. Such a system would allow an individual to be security-cleared up to a certain security classification level, rather than for a certain position. This would allow that individual to change roles within the same security classification level without the need for a new security screening process.

"In a global context, Sweden is almost unique in that we do not have a protective security clearance system. Should we adopt a new system, it is important to also retain the powerful tools that the current Swedish system provides, such as the security vetting interview and the continuous security screening carried out by the operator," says Oskar. ■

** Oskar is a fictitious name.*

The number of records checks and disclosures

In 2025, the Swedish Security Service received approximately 172,000 new requests to conduct records checks, which was an increase from 2024. The number also includes individuals checked along with the subject, that is, the spouse or partner of subjects to be employed in the security classes 1 and 2.

Information gained from a records check was disclosed to an operator on approximately 1,700 occasions in 2025.

A spy in our midst – finding an insider

One way for hostile foreign powers to gain access to valuable information is to recruit individuals who work where the information can be found. In order to detect such insiders, employers must carry out ongoing protective security efforts and establish a strong security culture in the workplace.

It is unusual that an individual would take a job for the purpose of infiltration. More commonly, people become insiders during the course of their employment. An employee who has come into financial trouble, is disappointed with their employer, or has fallen victim to an addiction can be more vulnerable to be recruited by an adversary hoping to gain access to critical information. Employers must ensure they have a good working environment, adequate personal information about their staff, and routines in place to detect changes and problematic contacts in their employees' lives, for example through regular conversations. Employers must also regularly review authorisations and access to security-sensitive information, as workplace responsibilities can change over time. The protective security measures must be ongoing and permeate the entire organisation.

While the following example is based on real events, the Infrastructure Authority is a fictitious government authority. The example highlights what an operator can do to stop an insider. ■

New job

Alex is a 40-something professional with good credentials who has sought employment at the Infrastructure Authority. The position is placed in a security class, and Alex will be involved in security-sensitive activities – in other words, work that is of importance to Sweden's security at a national level. Prior to Alex being hired, the employer therefore carries out a security screening to examine Alex's loyalty, reliability, and vulnerabilities.

Adverse findings in regards to loyalty are, for example, anti-democratic ideological convictions or problematic links to a foreign country. In terms of reliability, the screening aims to sift out individuals who are generally careless or have a pragmatic approach to rules and regulations. Vulnerabilities may arise down the line, and are not always something a person can control, such as if a relative has adverse contacts.

The Protective Security Act

Because Alex's new employer, the Infrastructure Authority, is involved in security-sensitive activities, it is subject to the Protective Security Act. This Act states that such operators must protect themselves pursuant to certain requirements, and take measures in three different categories: physical security, information security, and personnel security.

Physical security includes protective measures against trespassing and sabotage, such as fences, security guards, and locks. Information security concerns safeguarding critical information and essential systems that must always be up and running. Personnel security entails making sure that the staff is suitable from a security perspective.

Security screening

In the basic security screening, the employer examines certificates, grades, and references, and carries out a security vetting interview. Nothing emerges during this screening to indicate that Alex would be disloyal, unreliable, or be vulnerable from a security perspective. The Infrastructure Authority also requests a records check from the Swedish Security Service. Since Alex's position is placed in security class level 2, the Swedish Security Service conducts an enhanced security screening which delves deeper into Alex's life. Due to the security class level of the position, this also includes a screening of Alex's live-in partner. Everything appears to be in order, and the employer approves Alex.

The employer appears to have a solid process for security screening in place. Another important aspect is that employers are aware of which positions are engaged in security-sensitive activities, so as to avoid failing to conduct a security screening for certain positions.

Protective security analysis

In order to determine which aspects of their operations are security-sensitive, the Infrastructure Authority has carried out a protective security analysis. They are legally obliged to do this according to the Act. The analysis shows which areas of their operations require protection, and which measures are needed: what must be protected, against what, and how.

It may be that certain aspects or specific information are critical, and without a correct analysis, protective measures may be misguided or insufficient. Many operators find it difficult to identify their critical assets, which is problematic, as all protective security efforts are designed to protect that which has been identified as critical.

Protective security training

Immediately upon starting the new position, Alex is enrolled in protective security training, which is another important part of the Infrastructure Authority's personnel security efforts.

The training aims to raise awareness of protective security and to foster a security-focused culture to ensure that employees follow established procedures and regulations.

A balanced private life

The years pass, and Alex is performing well at the authority. Alex's family has grown and now also includes two children. The family's finances are in order, and Alex has been made chairperson of their housing association. In brief, Alex is doing well and is at a good place in life.

Critical assets

In this new position, Alex will have access to both security-classified information and other critical assets:

The position is located in a command centre that must always be operational. This means that it is security-sensitive from an accessibility viewpoint.

It is also an information system that must be functional, and the information therein must be correct. It is thus security-sensitive both in terms of accessibility and correctness.

Alex is also granted access to security-classified information in an internal information system, which must not end up in the wrong hands. It is security-sensitive from a confidentiality standpoint

Vulnerabilities

Suddenly, life takes a turn when Alex's partner walks out of their relationship. Alex is devastated, feels abandoned, begins drinking heavily and stops going to the gym. At work, Alex talks about the separation, but gives very few details as it feels too personal.

While there are things that should remain private, this is a situation that gives rise to new vulnerabilities. In addition to how a separation affects a person's well-being, it also often has a negative effect on a person's finances. Hostile foreign powers that want to get access to information on an authority, often attempt to find a way in through employees like Alex.

Friends

Alex receives a connection request on LinkedIn from Robin, who works in the same field. They begin chatting, meet up for lunch, and start spending time together. Before long, Alex has a new close relationship. After a night out with Robin, Alex oversleeps and is reprimanded by a manager in front of a group of co-workers. Shortly thereafter, a colleague is given a promotion that Alex had been hoping to get. Alex begins to feel unhappy at work and disappointed in the employer. Robin, meanwhile, is very affirming, interested in Alex's work, and asks a lot of questions, which Alex really likes.

Security screening – again

The employer has also failed to detect that Alex has new vulnerabilities. A continuously ongoing security screening process provides solid protection against insiders. Security screening must take place on a continuous basis, such as immediate supervisors asking their employees about their personal lives and not only focusing on work during follow-up conversations and performance reviews.

The goal is for the supervisor and employee to have a relationship where the employee, at an early stage, informs their supervisor if anything changes in their private life. It is important that the relationship between the employee and their supervisor is trusting and open. But even with the operator's shortcomings in this regard, the leak could have been avoided if the operator had conducted a thorough analysis of its critical assets and protected the information stored in the open-access system.

Information system

One day, Robin asks Alex to look something up in one of the Infrastructure Authority's IT systems. Alex, who no longer finds much enjoyment in the job, does not find the request odd. The information is stored in a system to which all employees have access and which is not subject to any particular protection. Alex finds this a bit strange, but sees no risks in doing Robin this favour.

The authority's protective security analysis has failed to identify that this system contains security-classified information. This information should be subject to a proper authorisation procedure and not be openly accessible. Such systems must also be equipped with security log monitoring, to be able to trace who has accessed what information.

A security-focused culture

It is management's responsibility to place the position of head of protective security at a strategic level in the authority and to ensure that security matters are always at the forefront. Processes, methods, procedures, and organisational systems must be permeated by a high level of security awareness.

The Infrastructure Authority should also strive to establish an enhanced security culture at their workplace. The difference between sufficient and insufficient security can come down to the people whose work involves security-sensitive activities and how they act in different situations.

Managers at various levels must serve as role models and comply with all aspects of the regulatory framework. An organisation with a robust security culture would allow for Alex's supervisor, or someone else at work, to be a person with whom Alex could share personal problems. Additionally, in such an organisation, anyone who discovers that information is stored in the wrong system would immediately report it. This would have stopped the leak. It should be easy to do the right thing, but it should also be okay to make mistakes, in the sense that employees should feel safe to point out shortcomings or problems with security in order for the organisation to remedy these oversights.

The threat of and protection against subversion

Detecting, preventing, and countering subversive threats is an important aspect of the Swedish Security Service's remit. The subversive threat refers to activities that ultimately aim to overthrow the democratic system.

The subversive threat refers to activities that aim to seriously undermine Sweden's basic democratic functions and values. While isolated incidents and crimes in themselves can be detrimental to the democratic system, such activities can only be regarded as a subversive threat when they are carried out systematically in a manner that, in the long term, could undermine the social order.

For an activity to be regarded as a subversive threat, both intent and capability are required. Examples of such activities are separatism, disruptive actions, and infiltration of critical infrastructure. Often, several of these methods are combined with a view to covertly bringing about the collapse of society, which is the ultimate goal.

There are organisations and networks in Sweden that, in the long term, could pose a serious subversive threat.

The protective work against subversion spans all the Swedish Security Service's operational areas, because this threat arises from various contexts and is manifested in different ways.

The Swedish Security Service's counter-subversion efforts

The remit of the Swedish Security Service involves detecting, preventing, and countering subversive activities in Sweden, regardless of whether the threat is posed by an individual, group, or state.

Intelligence gathering is an important aspect of the Swedish Security Service's counter-subversion efforts. This involves identifying potential threats, assessing the intent and capability of actors, and taking action against activities that pose a concrete subversive threat.

Sweden's democratic system, which the Swedish Security Service plays a significant role in protecting, encompasses extensive rights and freedoms, including the right to hold subversive opinions. The Swedish Security Service takes reduction measures only when actual activities that are assessed to have the capacity to pose a subversive threat or cause subversive harm take place.

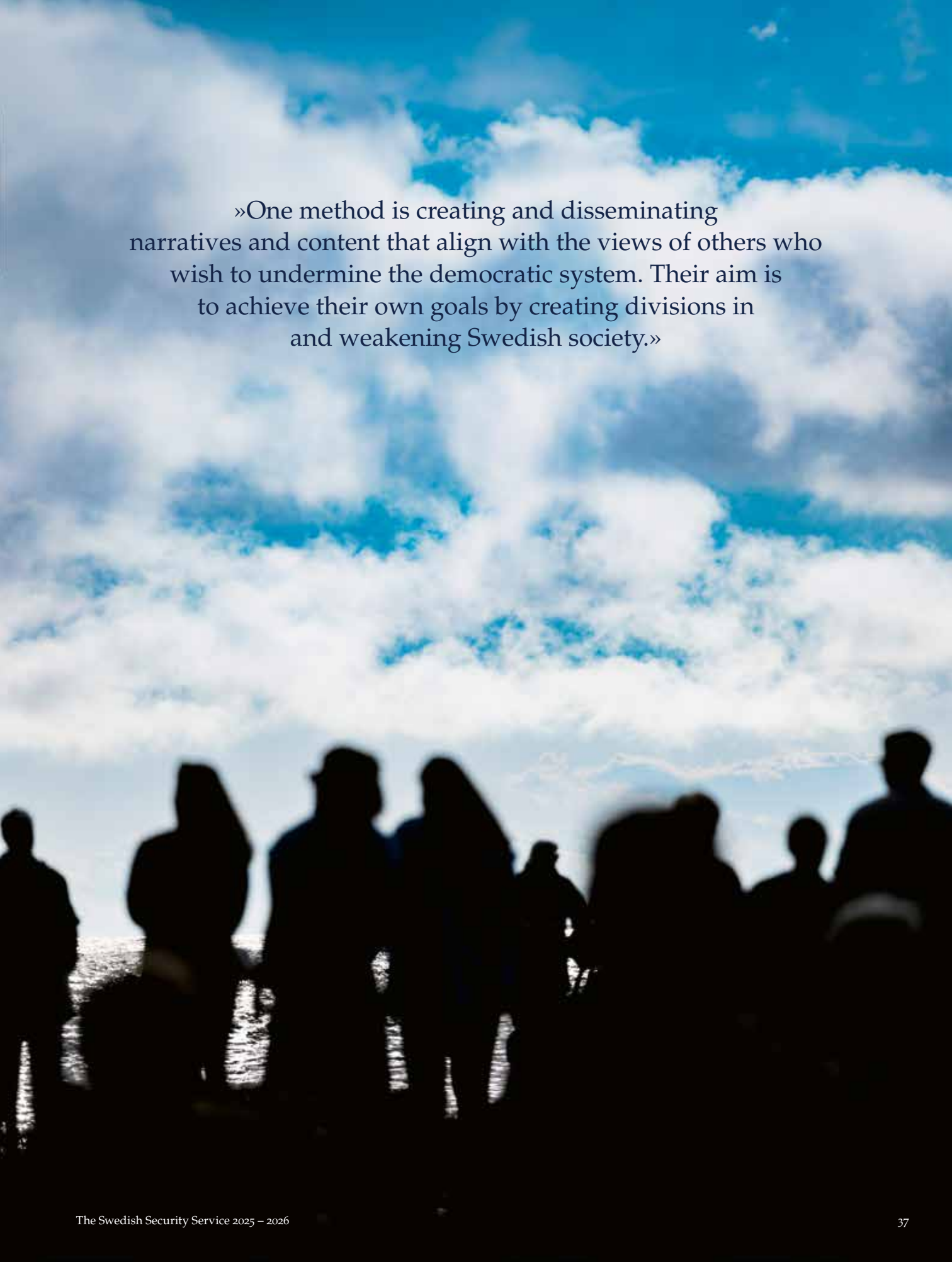
Subversive threat to Sweden

The most serious subversive threat to Sweden is assessed to be posed by organisations and networks that covertly carry out their activities with the aim of achieving long-term goals. The motives could be ideological, personal, or financial. Regardless of the motive, the threat posed by the subversive activities is assessed based on the harm that they would cause if carried out successfully.

The Swedish Security Service's current assessment is that there are actors who have the intent to carry out subversive activities, but who do not have the capability to pose a concrete and serious threat. Their capability could change however, and the Swedish Security Service therefore constantly monitors and analyses developments in this context.

Hostile foreign powers that fuel the threat

Hostile foreign powers – at present mainly Russia – have an interest in destabilising Swedish society by actively exploiting already existing subversive currents in our society by reinforcing them. Another method they use is creating and disseminating narratives and content that align with the views of others who wish to undermine the democratic system. Their aim is to achieve their own goals by creating divisions in and weakening Swedish society. ■



»One method is creating and disseminating narratives and content that align with the views of others who wish to undermine the democratic system. Their aim is to achieve their own goals by creating divisions in and weakening Swedish society.»

Cyberattacks require extra focus on security protection

Cyberattacks are happening all the time, targeting both private and public entities. Developments in technology entail that the methods used to carry out these attacks are constantly changing, and are becoming more and more accessible. The attackers may be hostile foreign powers, or a different type of actor, such as criminal groups that are motivated by financial gain.

Hostile foreign powers are interested in carrying out cyberattacks in order to gain access to information related to Sweden's national security, policymaking, or some other exercise of public authority. This means that authorities and political decision-makers may become targets for such attacks. Hostile foreign powers could use the information to identify vulnerabilities, or to attempt to influence policy-making, or also to initiate instability and stoke concern.

Cyberattacks are also conducted by actors who are mainly motivated by financial or ideological reasons, and who have no connection to hostile foreign powers.

Prioritising protection is important

Technological developments over recent years have led to methods which are more easily-accessible, and an increased capability for actors to carry out cyberattacks. Usually, the attackers take advantage of known technical vulnerabilities, for which, more often than not, fixes are available, but the user simply has not made the necessary security updates. More advanced attackers also have the capability to identify lesser-known or completely unknown vulnerabilities, taking advantage of these to conduct attacks.

»Developments in Sweden, and worldwide, show how complex and difficult it is to assess these threats and how they increasingly overlap and intertwine.«

The Swedish Security Service has noted that many IT incidents occur due to a lack of basic cyber security. There is a general need to increase the level of security-awareness of the operators, and that management at these entities also prioritise and allocate sufficient resources for working with cyber security issues. This would create a solid base to build a more suitable type of protection.

Collaborating for cyber security

The Swedish Security Service cooperates with other authorities at the National Cyber Security Centre (NCSC), through which the cooperating authorities manage IT incidents and suspected cyberattacks, and, when necessary, allocate responsibility amongst one another. Initially, it is often difficult to fully understand exactly what has happened, and who is behind an attack. Cyberattacks fall within the remit of the Swedish Security Service when the matter involves security-sensitive activities or if it is suspected that a hostile foreign power is behind the attack.

It is more common that IT incidents have no impact on security-sensitive activities, and that no hostile foreign power is suspected of involvement. Instead, these are crimes where criminal actors are motivated by financial gain, and in these cases, the Swedish Police Authority runs the criminal investigation.

Regardless of the underlying cause of a cyberattack, the Swedish Security Service can use the information from the incident in various ways, such as in intelligence-gathering efforts, creating situational assessments, or for gaining a better understanding of vulnerabilities, modi operandi, and threat actors. The Swedish Security Service can thereby improve how its interventions and measures are directed, and work strategically by developing guidelines and reviewing regulations on protective security. In the long term, this enhances the protection of Sweden's security.

Incident reporting is essential

In order for the Swedish Security Service to gain an oversight of the situation and identify common deficiencies, it is essential that entities working with security-sensitive matters report security-threatening incidents and activities.

These reports provide the Swedish Security Service with a better understanding of vulnerabilities, modi operandi and actors, and contribute to the efforts aimed at raising awareness of how operators can improve their security protection. ■

Obligatory incident reporting within security-sensitive operations

An operator must submit a report as soon as possible to the Swedish Security Service if:

- any classified information may have been disclosed
- certain types of IT incidents have occurred
- the operator becomes aware of or suspects any serious security-threatening activity.

Case:

What does the Swedish Security Service do in the event of a suspected cyberattack?

In this fictitious example, a municipal water company has been hit by a suspected cyberattack. For the Swedish Security Service, there are two key questions: Does the damage affect security-sensitive activities, and is a hostile foreign power behind the incident?

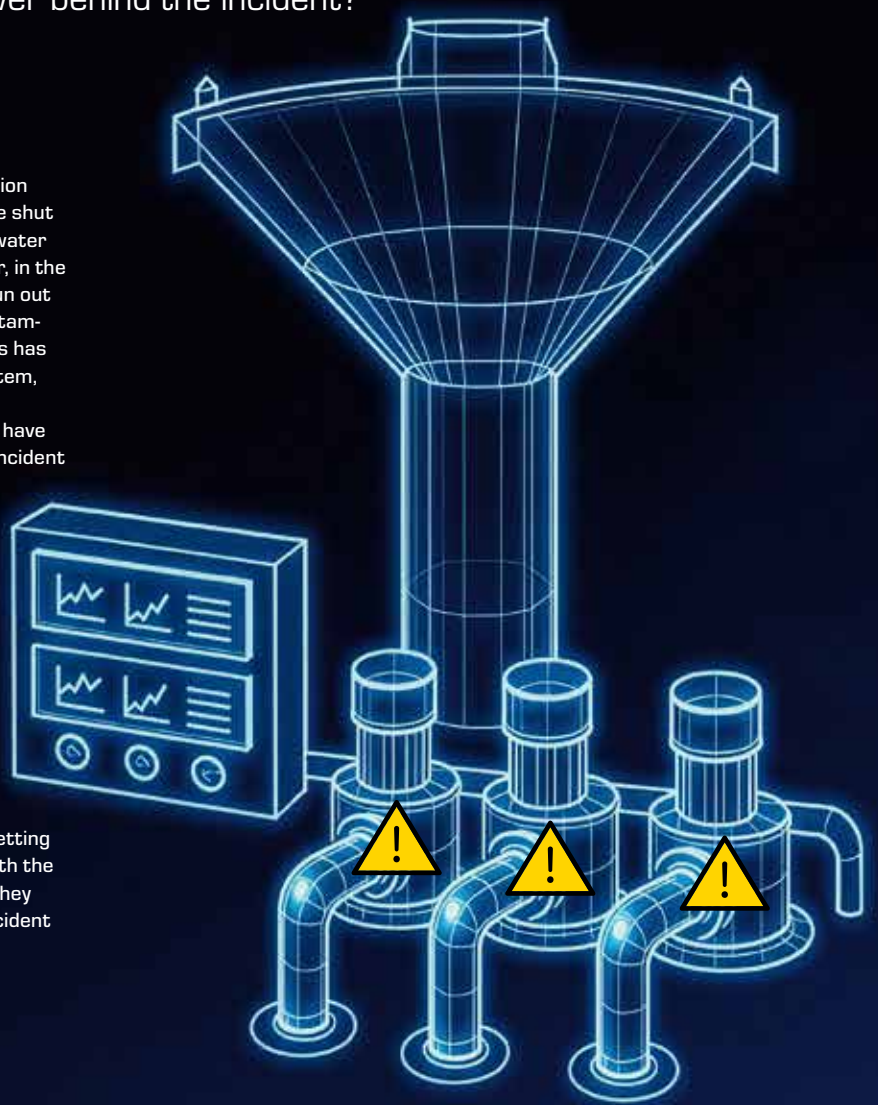
Scenario

The municipal water company in a certain region discovers one morning that their pumps have shut down completely. While the reserves in the water tower will be sufficient for a little while longer, in the not-to-distant future, the municipality may run out of water. The staff note that some technical tampering with the control system for the pumps has occurred. They are unable to access the system, and have to run the pumps manually.

It turns out that several pumping stations have been affected. The municipality reports the incident both to the police and to CERT-SE, Sweden's national Computer Security Incident Response Team, which supports Swedish society in managing and preventing IT security incidents.

The collaborating authorities at the National Cyber Security Centre (NCSC) are informed, and they, in turn, share information, assess the nature of the incident, and determine which entities can assist, and how.

The municipality bears the responsibility of getting the system up and running again, possibly with the assistance of contracted suppliers, though they may also receive support in managing the incident from CERT-SE, for example.



The Swedish Security Service gets involved

The Swedish Security Service determines how it can provide assistance, and assesses whether the incident falls within its remit. This would be the case if security-sensitive activities have been affected, i.e., either critical infrastructures are involved in such a way that Sweden's security is impacted at a national level, or if it is suspected that a hostile foreign power may be behind the incident.

In order to make its assessment, the Swedish Security Service gathers intelligence, and maintains an ongoing dialogue with CERT-SE, the authorities at the NCSC, and with the affected water company.

Have security-sensitive activities been affected?

→ The water company may be conducting security-sensitive activities, for example, it may be supplying one of Sweden's largest cities with water. The water company may also be providing services to other entities engaged in security-sensitive activities, for example, by enabling the functioning of cooling systems in critical data centres.

→ If the incident involves security-sensitive activities, the operator must submit a report to the Swedish Security Service. The Swedish Security Service processes this report, and, if needed, collaborates with affected actors, and assesses if any additional measures must be taken.

Are hostile foreign powers involved?

→ If there is indication of a hostile foreign power being behind the attack, the Swedish Security Service takes steps to further investigate the matter, including gathering intelligence. This information will then be used by the Swedish Security Service as part of its efforts to improve protection, and to prevent new attacks targeting Sweden. It can be difficult to link an attack to a hostile foreign power, as they may have used proxies, and operate in such a way that afterwards the hostile foreign power can plausibly deny any involvement.

→ The Swedish Security Service also investigates cyberattacks linked to its other areas of remit, for example, a data breach linked to terrorist-related activities.

→ It is more common that cyber incidents such as DoS attacks are linked to crimes investigated by the Swedish Police Authority, who then continue to work on the matter as part of a criminal investigation.

→ The Swedish Security Service also continuously monitors hostile foreign powers in order to detect cyberattacks which may not have been flagged as an incident.

CERT-SE is Sweden's national Computer Security Incident Response Team (CSIRT), tasked with managing and preventing IT security incidents occurring at organisations both in the private and the public sector. When an IT security incident occurs, CERT-SE disseminates information and supports the affected organisations in resolving or mitigating the effects. They cooperate closely with the NCSC.

The National Cyber Security Centre (NCSC) is tasked with developing and strengthening Sweden's overall ability to prevent, detect and manage hostile cyber threats and other IT incidents. The Centre is located at the National Defence Radio Establishment, and it is here that the Swedish Security Service collaborates with many other authorities such as the Swedish Defence Material Administration, the Swedish Armed Forces, the Swedish Civil Defence and Resilience Agency, the Swedish Police Authority, and the Swedish Post and Telecom Authority.

The threat of attack associated with violent extremism

The threat of attack to Sweden stems mainly from violent Islamism and violent right-wing extremism. However, there are also indications that violence itself may be a powerful driving force.

Digital platforms – a hotbed for the radicalisation of young people

Digital platforms are an important channel used for recruiting and radicalising children and young people. Violent propaganda and extremism are spread in order to radicalise the recipient. This occurs most frequently when a young individual:

1. Is exposed to violence and propaganda, e.g., through social media or gaming platforms.
2. Actively searches for propaganda and violent content on online forums. This could occur either alone or through contact with others.
3. Takes part in anonymous online forums. Contacts with like-minded individuals are formed, and one's own world view gets distorted. Fascination for violence is a unifying element in the group, and is also a strong driving force. Violence and extremism are normalised.
4. Adopts an extreme and violent world view. Violence is encouraged and justified by like-minded individuals.

On 23 May 2025, the Head of the Swedish Security Service decided to lower the terrorist threat level in Sweden from high to elevated, i.e., from Level 4 to Level 3 on a five-level scale. An elevated threat level includes the possibility that a terrorist attack could occur in Sweden.

The threat of attack is mainly associated with lone actors or small groups that act against accessible targets using relatively simple means. The intent to commit a terrorist attack can often be traced back to a specific incident or circumstance, either real or perceived, which serves as the triggering factor. The threat stems primarily from violent Islamism and violent right-wing extremism.

However, the Swedish Security Service has also noted a trend in which violence itself could be considered more important than ideological driving forces. This implies that individuals are more inclined to move between various groups and contexts that advocate the use of violence. Such mobility has also led individuals to increasingly design their own ideologies based on the contexts in which they find themselves.

The internet is an obvious platform for attracting and radicalising new supporters into violent extremism. Propaganda and gross violent content meant to normalise violence, and thereby lower the threshold for the use of violence, is spread in social media, on gaming platforms, and in closed forums. An individual's vulnerabilities, such as social exclusion or mental health problems, are factors that could affect the radicalisation process.

Due to the rapid dissemination of propaganda online, an incident in another part of the world could have an almost immediate effect on the threat to Sweden.

The threat from violent Islamism

In Sweden, violent Islamism consists mainly of facilitation activities by way of radicalisation, recruitment, and financing. While violent Islamism encompasses a variety of ideologies that have somewhat different objectives, the ideas of global jihad and an Islamist caliphate are very common.

The amount of threat-inducing propaganda that highlights Sweden as an anti-Islamic country has declined in the last few years. This is one of the reasons why Sweden is no longer regarded as a prioritised target for attacks, but is instead considered a legitimate target as part of the West. There are, however, examples where radicalising and violent rhetoric related to various international developments has been disseminated quickly with the help of the internet and has affected the threat to Sweden.

The threat of a terrorist attack stemming from violent Islamism is assessed to mainly be associated with young, lone actors who have been radicalised online and who plan to carry out attacks on accessible targets using simple means.

International developments also affect the threat that stems from violent Islamism. War and conflicts, above all in the Middle East, have been particularly threat-inducing in recent years. These types of developments are also exploited by international terrorist organisations for the purpose of raising funds and mobilising other kinds of support.

The threat from violent right-wing extremism

The violent right-wing extremist environment in Sweden is characterised by great variation and differing objectives. This could potentially attract individuals with different backgrounds and driving forces to join right-wing extremist contexts.

Although there are some relatively established organisations within the violent right-wing extremist environment in Sweden, the growth of this environment takes place mainly in loosely bound networks and groups online.

In spite of its great variation, common elements of the violent right-wing extremist environment include ideas about perceived race supremacy and survival, as well as various types of conspiracy theories. Another frequent element are accelerationist ideas, which embody the notion that society is headed towards a necessary collapse that should be accelerated through violence. A fascination for violence and previously committed attacks inspired by right-wing extremism are another recurring element.

The threat of a terrorist attack from violent right-wing extremism is assessed to mainly be associated with young, lone actors who have been radicalised online and who plan to carry out attacks on accessible targets using simple means.

In recent years, a number of violent attacks inspired by right-wing extremism have been conducted by young perpetrators in Sweden. None of these attacks have fulfilled the necessary criteria to be classified as a terrorist offence. However, an important remit of the Swedish Security Service is to monitor the environments of potential perpetrators in order to prevent and counter the likelihood that they will develop the intent and capability to carry out a terrorist attack or contribute to the growth of these environments by engaging in recruitment and radicalisation activities. ■

"The individual was arrested when the planning evolved into concrete attempts to construct an improvised explosive device".

The Swedish Security Service arrested a young man in Kungsträdgården, a park in central Stockholm, in February 2025. The man was there to carry out reconnaissance where he was planning to carry out a terrorist attack several months later with as lethal an outcome as possible. What he did not know at the time was that the Swedish Security Service had been monitoring him for over half a year.

"Thanks to successful intelligence and investigative efforts, the Swedish Security Service succeeded in averting an attack that could have caused serious harm. When we realised that his planning had evolved into concrete attempts to construct an improvised explosive device, we decided that the individual would be arrested," says Peter*, who works with counter-terrorism at the Swedish Security Service.

This case shows several ways in which the threat from lone individuals can be manifested. Radicalisation takes place relatively quickly, usually with the entire process occurring online. Large volumes of extremely violent content are consumed, which speeds up the radicalisation process. In today's propaganda, compared with the propaganda of a few years ago, violence features much more prominently than religious and political rhetoric.

Detecting and stopping lone individuals is a challenge for the security services in Europe.

"As a rule, these individuals have limited in-person contact with organisations and other individuals in the environment. Instead, the digital community is the main forum where they confirm each other's world views, dehumanise perceived opponents, and encourage the use of violence. There are often elements of mental health problems," says Peter.

This development entails that the Swedish Security Service must adapt its working methods.

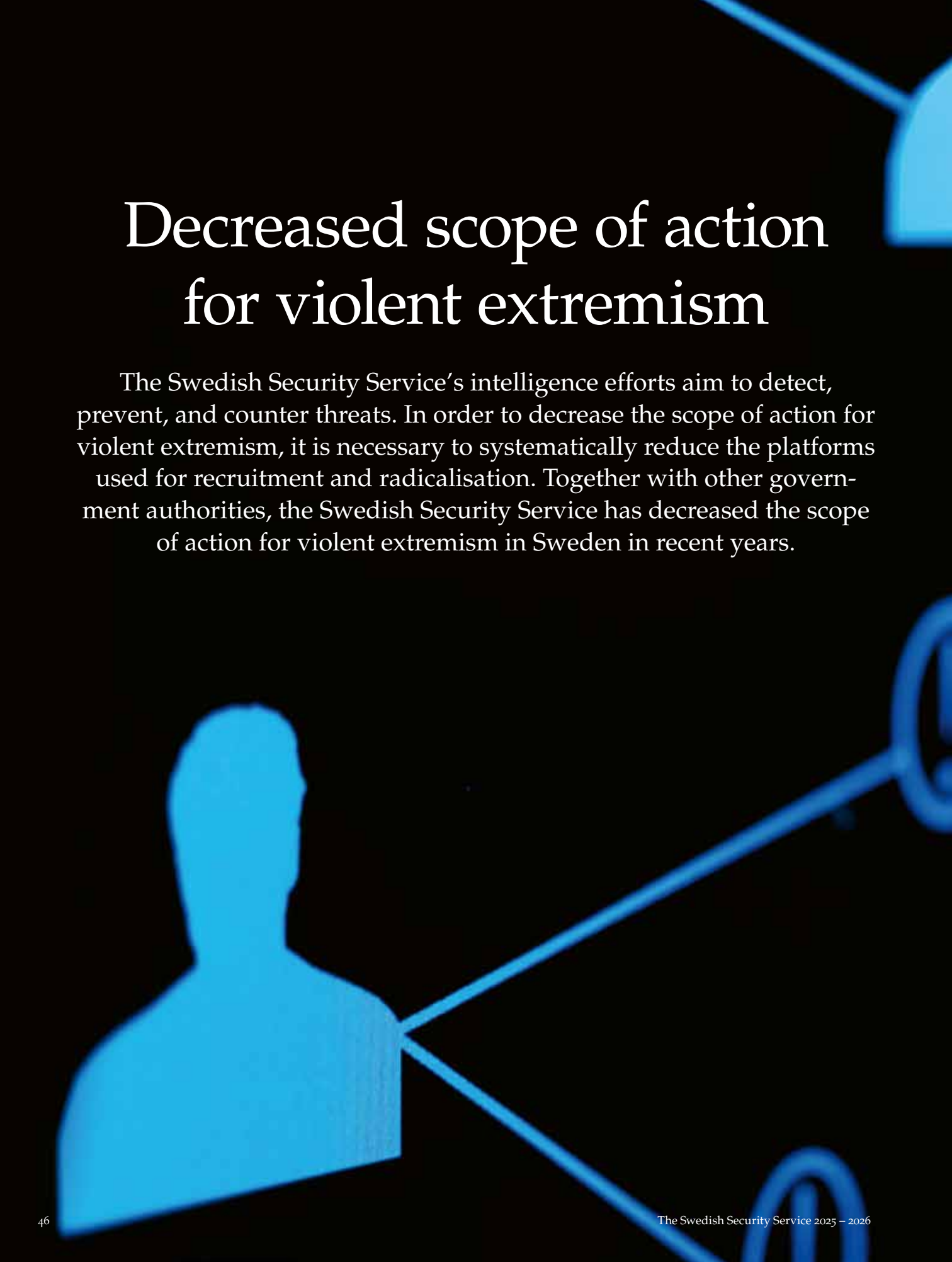
"We are constantly adapting our intelligence methods based on the type of threat we are dealing with and how it develops, which often requires both persistence and the ability to come up with new ways of working," says Peter.

The man was convicted by the Stockholm City Court in December 2025, and sentenced to seven years' imprisonment for several offences, including preparation to commit a terrorist offence, attempted murder, and gross offence against the Act on Flammable and Explosive Goods. At the time of writing, the final verdict has not yet been issued in this case. ■

** Peter is a fictitious name.*

Decreased scope of action for violent extremism

The Swedish Security Service's intelligence efforts aim to detect, prevent, and counter threats. In order to decrease the scope of action for violent extremism, it is necessary to systematically reduce the platforms used for recruitment and radicalisation. Together with other government authorities, the Swedish Security Service has decreased the scope of action for violent extremism in Sweden in recent years.



Fundamentally, it is about making Sweden an unattractive location for actors engaged in terrorist activities, regardless of their ideological motives," says Sofia*, who works with counter-terrorism at the Swedish Security Service.

Most of the Swedish Security Service's work is hidden from the public. This secrecy is necessary to successfully protect Sweden. The Swedish Security Service must keep its methods secret in order to remain effective, without those wishing to harm Sweden learning and exploiting how the Service works.

In some cases, the Swedish Security Service's efforts lead to judicial proceedings and convictions within the framework of terrorism legislation. While this is an important tool for reducing the terrorist threat to Sweden, it is far from the only one. As a security service, bringing people to justice is not our main remit – protecting Sweden is. For this reason, the Swedish Security Service always strives to detect and avert security-threatening activities as early as possible.

Changing working methods

In the past ten years, the Swedish Security Service's counter-terrorism efforts have seen significant changes. The number of threats of attack against Sweden and the rest of Europe was high during parts of the 2010s. A considerable part of the Swedish Security Service's efforts focused on detecting and averting concrete attack planning, either working on our own or together with international partners.

At the same time, there were several platforms in Sweden where violent extremist movements could

»In the past ten years, the Swedish Security Service's counter-terrorism efforts have seen significant changes.»

recruit and radicalise new attackers. The proclamation of the Islamic State caliphate contributed to their power of attraction and expansion. The need to reduce the platforms' ability to act in order to slow the growth of the extremist milieus became more evident.

The Swedish Security Service has taken several measures to prevent radicalisation and decrease the scope of action for recruitment in Sweden. One of the most important aspects in these efforts is the enhanced cooperation between Swedish authorities. In recent years, the Counter-Terrorism Cooperation Council and the national strategy to counter violent extremism and terrorism have become important tools in these joint efforts.

»We have become more open, and share more information with others. This is an important success factor for reducing and preventing violent extremism and terrorism.»

Extensive cooperation between authorities

The results of the Swedish Security Service's intelligence efforts have, to an ever-growing extent, given way to efforts by other government authorities to restrict the possibilities of committing terrorist offences in and against Sweden.

"The Swedish Security Service has spent significant time on improving cooperation with other authorities to obtain better results from our counter-terrorism efforts. We have become more open, and share more information with others. This is an important success factor for reducing and preventing violent extremism and terrorism," says Sofia.

Thanks to better inter-authority cooperation, the effective reduction measures have been prioritised, which, in turn, have reduced the possibility for violent extremist actors to take action. One example is the prioritisation of prosecutable offences over more complex or ideologically motivated crimes. Particular focus has been placed on preventing individuals who are active in violent extremist circles from abusing the social welfare systems, such as the social security system or the tax system.

"We have enhanced our cooperation with other authorities to allow for unified efforts to tackle the problem. In many cases where we cannot use terrorism legislation to prosecute an individual who is part of a radical extremist environment, that individual can be prosecuted for other criminal activities. As a result of our cooperation, other authorities are able to prioritise investigations regarding these individuals, thus making it more difficult for them to operate," says Sofia.

Stopping fraudulent welfare system payments has a double effect. It makes the actors less able to support themselves financially, and thereby less able to engage in terrorist-related activities. It is also important for directly preventing financing of terrorist activities, both in Sweden and abroad. Systematically exploiting the welfare system is a method to fund terrorism and the growth of extremist milieus.

Another tool for making it harder to conduct terrorist-related activities in Sweden is the legislation concerning foreign nationals – the Act concerning Special Controls in Respect of Aliens. Pursuant to this Act, individuals who are not Swedish citizens and who pose a serious security threat to Sweden can be expelled. The Swedish Security Service, together with the Swedish Migration Agency, uses this option to keep influential terrorist actors from exploiting Sweden as a platform for their activities.

"While we cannot enforce all expulsions, an expulsion order pursuant to the Act concerning Special Controls in Respect of Aliens makes it more difficult to operate in Sweden. These individuals may be subject to limitations in their freedom of movement, employment options, and receiving social welfare benefits," says Sofia.

Structural changes

Swedish government authorities have also cooperated to ensure that public funds are not used by, or in connection with, entities that promote radicalisation and undemocratic methods, such as schools or extremist religious associations that have served as platforms for recruitment.

"The Center for Preventing Violent Extremism (CVE) has also played an important role in the joint efforts to counter violent extremism. Their outreach activities have allowed the knowledge that we have obtained through our intelligence efforts to have a wide reach in society, on an aggregate level. The information campaigns they run in schools and at social welfare offices around the country have increased awareness, and thus the attention given to individuals who may be at risk," says Sofia.

The legislative developments have also allowed for judicial action to be taken more often. In recent years, several laws have been implemented for the purpose of countering terrorism more effectively. This includes preventing financing of terrorism, and travelling to and participating in terrorist organisations. These laws have been used on several occasions, and have limited the opportunities for actors in Sweden to support terrorism and terrorist organisations.

Limiting terrorist environments

The scope of action for violent extremist organisations that previously engaged in recruitment and radicalisation have been severely restricted.

"We can clearly see the results of our efforts. Engaging in radicalisation with the aim of having an individual commit a terrorist attack is considerably more difficult in Sweden today than it was ten years ago. The possibility for these milieus to operate has been severely reduced, and our efforts are more long-term and proactive, rather than reactive. However, we must remember that the threat can change rapidly. We must continue to monitor developments," says Sofia. ■

** Sofia is a fictitious name.*

Working together to secure the general election

Collaboration between authorities is key to ensuring that a general election can be conducted in a secure manner. It is the remit of the Swedish Security Service to discover, counter, and prevent crimes which target Sweden's national security.

Sweden has a fundamentally robust electoral system, featuring a transparent process which is difficult to manipulate. At the same time, however, there are hostile actors who have an interest in weakening the Swedish democratic system.

The Swedish Security Service, together with several other authorities, is responsible for ensuring that the general election is held in a secure manner, without any major disturbances. The Swedish Election Authority is tasked with coordinating the security around the general election. Several of the Swedish Security Service's standard missions, such as providing protection for the Central Government, and preventing hostile foreign powers or violent extremists from carrying out security-threatening activities, are also linked to the general election.

Sharing information

Several authorities work closely together to ensure that the general election can be carried out freely and democratically. The core element of this collaboration consists of a permanent national elections network for which the Swedish Election Authority is responsible. In addition to the Swedish Security Service, this network also consists of other Swedish authorities such as the County Administrative Board, the Psychological Defence Agency, the Swedish Civil Defence and Resilience Agency, the National Cybersecurity Centre, and the Swedish Police Authority.

Within this network, authorities can share information and situational assessments with one another. As the election day edges closer, cooperation intensifies.

Ensuring the security of protected dignitaries

The Swedish Security Service is responsible for the protection of the Central Government which includes the Prime Minister, Government Ministers, and Members of Parliament. Included in this responsibility is also the task of ensuring that the election campaign can take place securely.

The number of rallies, door-to-door canvassing, and other related activities increases dramatically during an election year, and in connection with this, so does the exposure and visibility of protected dignitaries, resulting in changes to the threat as well as vulnerabilities.

As an elected official with a high degree of visibility, their day-to-day life is considerably altered, and conscious decisions must be taken in order to increase their personal security. Collaboration is a critical component of the dignitary protection mission. In matters relating to the security of protected dignitaries, the Swedish Security Service works closely with the Swedish Police Authority, as well as with the security organisations of the Government Offices of Sweden, and the Swedish Parliament.

Threat actors and the general election

Hostile foreign powers have an interest in malignly influencing Swedish policymaking, and a general election can serve as an opportunity to carry out activities which promote the long-term interests of these powers. For Russia, this involves sowing discord within NATO, throttling support to Ukraine, and ensuring the survival of the Russian regime. By disseminating disinformation, a hostile foreign power can attempt to fuel conflicts in Sweden.

Sweden has a robust, legally secure, and decentralised electoral system. The electoral process is transparent, with several built-in systems of control in which the votes are counted manually, several times, at many different stages. This makes the system difficult to manipulate.

»The number of rallies, door-to-door canvassing, and other related activities increases dramatically during an election year, and so does exposure.»

Past experiences have shown that there is an increase in activity within the violent extremist milieus during an election year, and this is assessed to be the norm. This mainly pertains to violent right- and left-wing extremism, with activities primarily directed at individuals perceived to be ideological opponents. Currently, the Swedish Security Service has no indication of the general election itself being a designated target for these milieus, although the election year may be used to disseminate propaganda and attempt to entice new supporters. ■

Which authority is responsible for what?

The Swedish Security Service is responsible for making threat assessments and taking protective measures for the Central Government, including the Head of State, the heir to the throne, the Speaker of the Parliament, Members of Parliament, the Prime Minister, Ministers, State Secretaries, and the State Secretary for Foreign Affairs.
The Swedish Police Authority is responsible for making threat assessments and taking protective measures for all individuals who do not fall under the responsibility of the Swedish Security Service, such as local and regional politicians, journalists, and employees of the judicial system for example.

Dignitary protection in turbulent times

One of the remits of the Swedish Security Service is to provide protection for members of the Central Government, allowing them to carry out their duties in a secure manner. In a turbulent international environment, and when faced with a serious security situation, changes to protective security measures may be required.

The Swedish Security Service's Dignitary Protection Unit conducts a wide range of activities, and the means of providing protection for the individuals in the Central Government may differ on a case-by-case basis, or vary over time. Protective security measures are always based on a threat assessment, adapted to both general and specific situations, and take into account the specific vulnerabilities pertaining to different individuals.

"The planning and design of dignitary protection is based on a variety of tools and methods. Circumstances, however, can change rapidly, which require constant updates to assessments. One component of our security efforts is to intentionally be unpredictable, in an attempt to remain elusive," says Petra* who works as an Analyst at the Swedish Security Service's Dignitary Protection Unit.

»This may involve intelligence gathering, as well as giving advice, implementing physical protective security measures, and providing close protection and secure transportation.«

Dignitary protection includes a wide-range of measures. This may involve intelligence gathering, as well as giving advice, implementing physical protective security measures, and providing close protection and secure transportation.

"We never give out any details or comment on which protective measures apply to a specific individual. This is also a component of how we provide protection. The less a potential attacker knows, the more effective the protection," says Petra.

Serving as an elected Member of Parliament or as a Government Minister may entail significant public exposure.

"Such public exposure results in needing a completely different level of security-awareness compared to members of the general public. This means that life, in certain aspects, can change considerably," says Petra.

Cooperating with others is a key element of the Swedish Security Service's Dignitary Protection Unit. Our cooperation with the Swedish Police Authority, as well as the security organisations of the Government Offices, the Swedish Parliament, and the Royal Court is of particular importance. This creates a security awareness and a general consensus of the required protective security measures relating to the Central Government. ■

** Petra is a fictitious name.*

For more information on critical security-enhancing measures for elected representatives, please refer to the handbook on personal security, available at sakerhetspolisen.se/personlig-sakerhet (currently in Swedish only).

For more information,
visit www.sakerhetspolisen.se

Follow the Swedish Security Service on
Instagram and LinkedIn.

Production: Swedish Security Service
Graphic design: Intellecta
Photo: Swedish Security Service
Printed by: Ljungbergs tryckeri

ISBN: 978-91-86661-31-1
How to order: The publication can be downloaded from www.sakerhetspolisen.se or ordered via: sakerhetspolisen@sakerhetspolisen.se

The Swedish Security Service works to prevent and detect offences against Sweden's national security, counter terrorism, and protect the Central Government. We do this in order to safeguard Sweden's democratic system, the rights and freedoms of our citizens, and to protect national security.

Säkerhetspolisen
Swedish Security Service