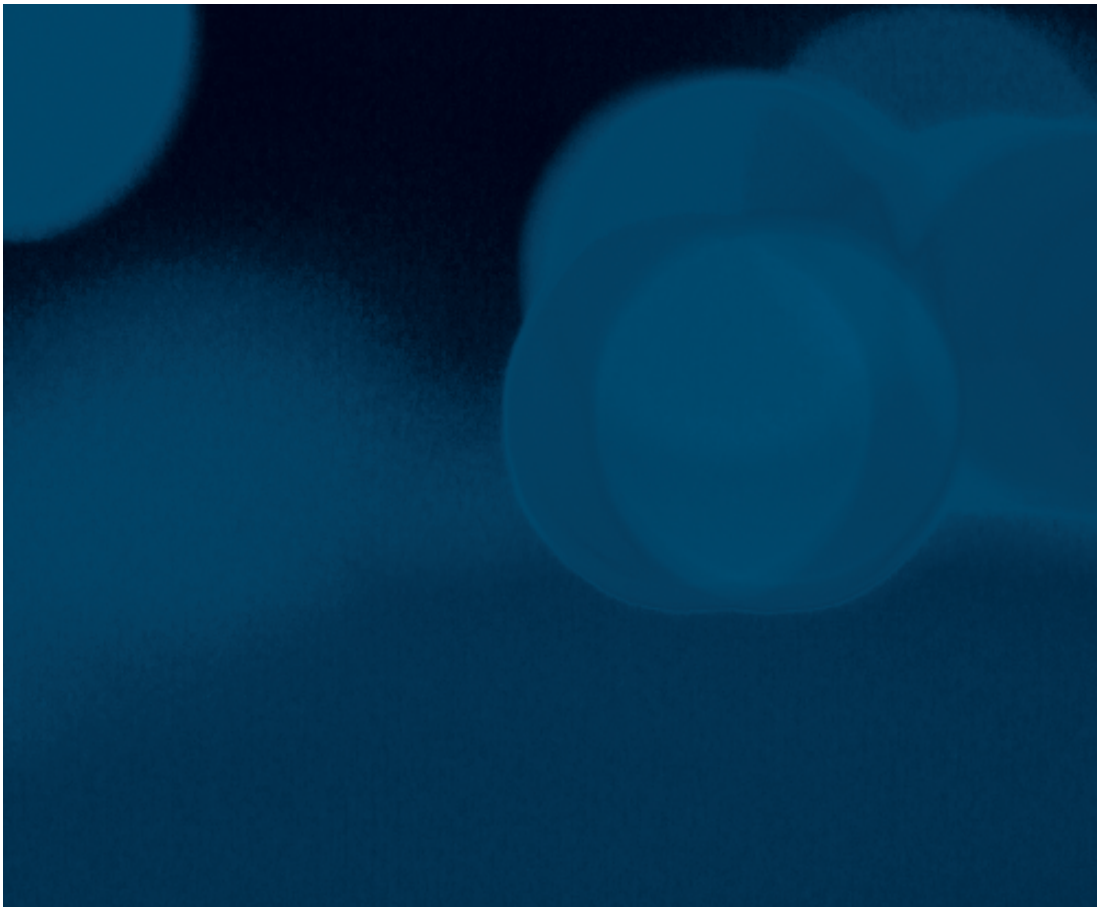
SUPO

National Security Overview 2025



THE GLOBAL SECURITY ENVIRONMENT AND FINLAND

2
A grim security situation has given intelligence a key role in foreign and security policy

6
China strengthens its presence in the Arctic

10
Russia is reorienting globally

12
Growing use of intra-EU supply chains in Russian sanctions-busting

17
Data may also be used for purposes that threaten Finland

ESPIONAGE AND INFLUENCING

20
Overview of state espionage and influencing

24
Russia seeks to influence European countries through sabotage

27
Authoritarian state cyber ecosystems endanger international stability

34
China is using social media platforms for intelligence gathering

TERRORISM

38
National Terrorism Threat Assessment 2025

42
Radicalisation of minors has become a persistent problem in Europe

44
Growth in reports concerning the radical far right in security clearance vetting

THE YEAR AT SUPO

46
The year 2024 through the eyes of six Supo employees

A grim security situation has given intelligence a key role in foreign and security policy

Juha Martelius
Director of the Finnish
Security and Intelligence Service

State and national security have returned to the core of political life. A gloomy era of superpower competition and confrontation between states has enlarged the role of security and intelligence services in foreign and security policy.

The growing importance of intelligence was also acknowledged in the Government Report on Finnish Foreign and Security Policy published last summer. It is important for the government to know what adversaries are planning, and to understand trends in the security environment. Verifying the absence of adversarial influencing is also essential, as mistaken assumptions, speculation and other such distortions may also emerge from ordinary public debate. Information of this kind is not usually available from public sources. Supo applies the full range of instruments allowed under intelligence legislation to secure intelligence on the trends that threaten our national security.

Proxies used by various states are playing an increasingly important role in both intelligence and broadly based influencing. Whether referring to Russia, China or Iran, state actors are seeking to cover their tracks by working through intermediaries. Such proxies enable power agencies of authoritarian countries to confuse the real state of affairs, lend plausible deniability to their actions, and foster new forms of uncertainty. Recruitment can be conducted through social media, with payment made in cryptocurrencies so that assignees need not even know who they are ultimately working for.

Russian sabotage operations in Europe are one example of the use of proxy actors. These operations have become increasingly dangerous, showing indifference to the safety of innocent bystanders. They cover a broad spectrum from highly complex cyberattacks to simple acts of destruction. Their main objective is to undermine Western support for Ukraine.

Finland has not been a target of strong Russian influencing so far. Such influencing has instead primarily targeted large EU Member States, and also countries with a substantial Russian minority or pro-Russian political parties.

The impression of Russian influencing conveyed in the media – and consequently in the public imagination – does not always reflect reality, with such incidents as ordinary domestic vandalism counted as actions taken by Russia. Russia is happy to see this, as it amplifies the deterrent effect and fosters an impression of Russian omnipotence.

Russian influencing operations continually test the West and NATO, monitoring their reactions and resilience. Russia understands the West and Finland poorly. For example, Finland's accession to NATO surprised the Russian leadership. A deteriorating understanding of the logic of Finland's actions, coupled with reluctance to convey unwelcome news to top-level leadership, may pose a risk of misjudgement leading Russia to react based on its own misinterpretations.

In an increasingly obfuscated arena, influencing also requires a growing input from the intelligence services. Supo seeks to warn the Finnish government of Russian non-military influencing in advance. Public authorities also use intelligence provided by Supo to mount an effective defence against the most serious threats, such as terrorism.

The rules of the intelligence world require extreme discretion, meaning that only like-minded services may be parties to international intelligence exchanges. This makes intelligence services invaluable tools for nation states. These doors will nevertheless be completely closed to Finland unless Supo and Finnish military intelligence are adequately resourced to assist in collaboration with foreign partners.

It is clear that Russia in particular has significantly altered our security environment, with no signs of improvement in sight. Russia is an aggressive, expansionist state that is prepared to use all means to achieve its political goals. Russia's emphasis on an imperialist character, factually unfounded historical interpretations, and a decades-long manipulation of the nation into believing in the historic mission of the country call for a capable and strong Finnish intelligence that can provide early warning of potential measures against Finland. ■

The global security environment and Finland

China strengthens its presence in the Arctic

The war of aggression has made Russia increasingly dependent on China, with these two countries stepping up their cooperation in the superpower competition for the crucial Arctic region.

Ice cover in August 2024

RUSSIA

MONGOLIA

CHINA

KAZAKHSTAN

GREENLAND

SVALBARD

Russian research station

Chinese research station

Chinese-Icelandic joint research station

Russia has over 50 icebreakers

China has 5 icebreakers

Polar circle

Northeast Passage

As a result of the sanctions imposed due to the war of aggression against Ukraine, Russia has become even more dependent on China. This new situation creates conditions for even closer cooperation between Russia and China in the Arctic. This cooperation has enabled China to gradually reinforce its presence in this part of the globe. Russia has become China's primary route to the Arctic region.

Increasing cooperation between China and Russia in the north is visible in many ways. Joint Russian and Chinese coastguard patrols were arranged in the Arctic for the first time in autumn 2024. These countries have also arranged joint military exercises in the Gulf of Finland.

Russia enjoys Chinese technological support and energy project investments in the Arctic region, where Sino-Russian research cooperation has also intensified.

Growing superpower competition in the Arctic has repercussions for Finland

The Arctic region is a key arena for superpower competition, and the growing presence of China in this region will probably boost this still further. As an Arctic state, Finland will inevitably notice any shifts in the local balance of power.

The mission of Supo as an intelligence service is to investigate trends of this kind that significantly affect the national security of Finland.

Any rapprochement between China and Russia will have a wide range of impacts on Finland. Russia views NATO as a direct threat, and China opposes all military alliances that include the USA. The Arctic region is important for developing, using, detecting and combating nuclear weapons and their delivery vehicles, and for the associated strategic balance.

The risk of Western expertise and technology reaching Russia via China has also grown. Finland has diverse Arctic expertise that is of interest to China and Russia. A detailed understanding of how to build icebreakers and other ice-strengthened vessels is merely one example of this.

The Arctic is a key region for satellite and other technology

The Arctic region is strategically important for reasons of security, trade and technology. We have long been aware that melting ice sheets will open up new sea routes and access to natural resources, such as minerals, gas and oil. As a superpower, China will seek to exploit these opportunities.

The Arctic region is similarly important for satellite technology, as the polar regions are an ideal location for ground stations. Many military and civilian positioning and communication systems rely on satellite technology.

While China has sought to establish ground stations in the Nordic region, these projects have drawn criticism from Finland and other Nordic countries. Finland has responded by making ground and radar stations subject to licensing. Current legislation also assesses licences from a national security perspective.

China also understands that a superpower must have a navy capable of operating at any location, including in Arctic conditions. China is seeking an independent Arctic operating capability in the long term, and has accordingly invested in developing its icebreaker fleet.

Russia needs China

The Russian war of aggression has had a significant impact on the dynamics of the Arctic region. While this impact has included paralysing the work of the Arctic Council, the most important change has concerned relations between China and Russia.

Even a decade ago, Russia was far more sceptical about Arctic cooperation with China, as it sought to maintain its own dominant status in the region. Even though China and Russia have similar goals, with their cooperation growing closer in recent years, the relationship is still characterised by distrust. China now has a stronger negotiating position in discussing Arctic cooperation with Russia than before the war of aggression.

The Russian military industry is highly reliant on technology imported from China, including microchips and various components. Russia is also increasingly dependent on China economically as Chinese support enables Russia continue its aggressive operations in Europe.

Russia should nevertheless not be underestimated. Russia remains the stronger actor in the Arctic region due to its long history, even though it must now tolerate more from China than before. It is telling that Russia has more than fifty icebreakers, while China has only five.

A strengthened Arctic presence is one of China's broader objectives

China is pursuing a global military presence overall, and so its interest in the Arctic is only part of a broader ambition in which the most important issue is superpower competition with the USA.

China benefits from securing a closer partnership with Russia in confronting the USA. It is seeking to reinforce international structures that are independent of the West, with growing cooperation between the BRICS countries serving as one example of this.

Russia also benefits from this reinforcement, even though it is clearly led by the Chinese.

China has no desire to jeopardise a good bilateral relationship by applying heavy pressure on Russia, whose stability frees up Chinese resources for its primary aim of pursuing superpower competition with the USA. China may even allow matters to take their course, waiting until Russia has to request assistance. ■

Russia is reorienting globally

Though posturing aggressively towards Europe, Russia would like to restore trade relations with European countries. Its key global objectives are to undermine support for Ukraine and to alleviate the current regime of sanctions. Russia is also now looking in new directions.

Three years of war in Ukraine have forced Russia into a significant international reorientation. Even though Russia projects confidence in its foreign policy, it is evident that its importance has declined globally.

The shift has been most dramatic in the collapse of relations between Russia and the West. The conduct of Russia has significantly reduced its influence in Western countries.

With a decline in customary channels of influence, Russian actions in Europe have grown more aggressive. The ability of the West to influence Russia has similarly waned as relations with the Russian people have grown more distant.

This repositioning significantly magnifies the risk of misunderstandings and overreaction. With an almost complete break in traditional diplomacy, discussions have increasingly shifted to the public domain. A lack of information through conventional channels increases the need for intelligence on both sides.

Russia looks to the East and the South

Russia is nevertheless not as globally isolated as might appear when viewed from the West. Its most important line of sight is now towards China. Russia has increasingly tied itself to China, and to Chinese foreign policy objectives. It is evident that China is the more powerful party in this relationship. Russia and China are seeking to strengthen international structures in which Western countries are not involved.

Russia is looking to the global South, meaning Africa, Asia and Latin America. Cooperation between the BRICS countries is one aspect of this. While seeking to explore trade projects in the global South, Russia also aims to increase its political clout, as is evident in its diplomatic and other efforts.

The global South will clearly not replace the European market that was previously a target for a large part of Russia's international trade. This is partly a matter of basic logistics: gas pipelines to new locations cannot be constructed overnight.

Russia does not have an open playing field, even in the global South. The Wagner mercenary group previously served as a channel of Russian influence in several African countries, but the Russian Ministry of Defence has now disbanded Wagner in the wake of a coup attempt in summer 2023. The rigid bureaucracy has been unable to replace the company, which operated as a more agile channel of influence. This means that Russia has become less influential in Africa.

Russia takes an aggressive posture, but would like to restore trade relations with Europe

Russian President **Vladimir Putin** has now been in power longer than any European leader, giving him a certain degree of confidence. With no need to consider election cycles in planning, the Russian leadership believes that a policy of attrition may be effective in many issues.

The key goal of Russian influencing is to undermine support for Ukraine. Russia may be considered to have partially succeeded in this respect, as it has been able to effect constraints on military support provided by the West. On the other hand, Western support for Ukraine has continued and become more established as the war has dragged on.

Despite conveying a rhetorical impression of confidence and aggression, Russia would like to restore trade relations with European countries. Another key objective for Russia is to see some lifting, or at least easing of sanctions.

Russia seeks to address its message in Europe to listeners who would like normalise trade relations. While support for Ukraine has been quite unanimous in Finland, attitudes are not so clear in many other European countries. Russian influencing seeks to focus on economic arguments.

The worldview of the Russian leadership does not regard all Western countries as absolutely evil, but draws a distinction between the good West and the bad West. Western leaders are cast as the bad West, which seeks to isolate Russia. By contrast, the good West is represented by ordinary people, and by those who would be willing to continue trading with Russia. Russia does not value democracy, or the fact that political leadership in European countries reflects the views of the people.

Clearly there is no going back to business as usual in trade relations between Europe and Russia from either point of view. Restoring trust in the eyes of Europeans would require a radical and unlikely change in Russia, but Russia, in turn, has no desire to become as dependent on the West again as it was before the war.

Small states not crucial for Russian influencing

Russian influencing in Europe focuses particularly on large countries, and naturally also on Ukraine. Russia is not an omnipotent influencer, but a country at war that must prioritise its actions. Small countries like Finland are not the most important influencing targets from Russia's perspective.

Russia views itself as a superpower that is primarily opposed to the USA. On the other hand, Russia also feels itself to be under threat, and to be acting reciprocally, even when escalating the situation from the perspective of the West. Its key objective is to maintain its own internal stability.

While Russia remains the greatest threat to Finland, we are not as important from the Russian perspective, which views small countries like Finland as a zone of operations that serves the interests of major powers. Russia envisages a world in which small states should become satellites of larger states that may disregard their interests when a few large countries settle matters between themselves.

At the same time, the Baltic Sea has major significance to Russia. A shadow fleet navigating the Baltic Sea is currently the most economically and logistically viable option for Russia to transport oil by sea. Using this shadow fleet to evade sanctions on crude oil is very important to the economy of the Russian Federation.

It is evident that the relationship between Russia and Finland has shifted fundamentally. Russia views Finland as an unfriendly country due to its NATO membership and other factors. It feels that Finland has betrayed its trust by becoming an ally of the USA.

Russia continues to prepare for a deepening confrontation with the West, and is striving to maintain instruments that it can resort to if necessary. It is preparing for various hostile operations against Western countries, and also against Finland. Such preparations nevertheless do not indicate that any decision has been made to take such actions immediately. ■

Growing use of intra-EU supply chains in Russian sanctions-busting

The methods applied by Russia to evade sanctions and export restrictions are becoming increasingly hard to identify, and businesses may unwittingly be involved as procurement routes grow more complex.

Russia is continually seeking new and more subtle ways to circumvent sanctions and export restrictions, with procurement increasingly concatenated within the EU internal market also.

Russia's aim is to conceal supply chains more effectively as Western authorities become increasingly aware of its schemes to evade sanctions and export restrictions. The growing number of supply chain intermediaries makes it increasingly difficult for public authorities and enterprises to identify their ultimate business partners.

The extension of a supply chain into the EU internal market means that Finnish business contacts may come from Finland or from another EU country. No clear connection to Russia or to some non-EU country may be evident in such contacts.

Procurement chains use both individual enterprises and broader procurement networks as a front behind which Russia can secure access to required materials.

Chains that begin in the EU internal market often continue into third countries via some long chain of intermediaries.

The impact of sanctions is visible in Russia

Russia seeks to evade sanctions and export restrictions in order to procure the products and technology that it needs.

Finnish businesses, universities and research institutions have a great deal of internationally recognised expertise and sophisticated technology. Russian procurement efforts may target both cutting-edge technology and conventional components, such as printed circuit boards. Items of particular interest include various electronic components, measuring instruments, machine tools, materials technology, optics, maritime technology and quantum expertise.

Dual-use items subject to export control under an EU Regulation are also on the Russian procurement list. Dual-use items are technology or products with both civilian and military applications, or that can be used for developing weapons of mass destruction.

The sanctions and export restrictions imposed on Russia hamper and delay procurement of certain controlled products, and make them more costly. Russia needs these procurements in particular to maintain its military capability.

Attention should be paid to unusual contacts

Businesses may be unwittingly involved in circumventing sanctions and export restrictions as Russian procurement routes become more complex and increasingly linked to the EU internal market.

Enterprises should always pay particular attention to unusual procurement efforts or contacts. Such contacts may come from a business that was recently established, or is based in a country with a hitherto unfamiliar operating environment. This business may have a long history of trading with Russia, or it may have significantly modified its operations in such respects as exporting, importing and payment arrangements for purchases.

Enterprises should also be wary of business partners that only communicate through various intermediaries or authorised representatives. They should exercise caution with respect to unusual payment arrangements, such as those in which a buyer seeks to pay for a purchase through a third party, or using bank accounts based in tax havens. Effective contract management and good customer knowledge can help enterprises to reduce the risk of unwitting involvement in a network that evades sanctions or export restrictions.

Businesses are liable for complying with sanctions and export restrictions

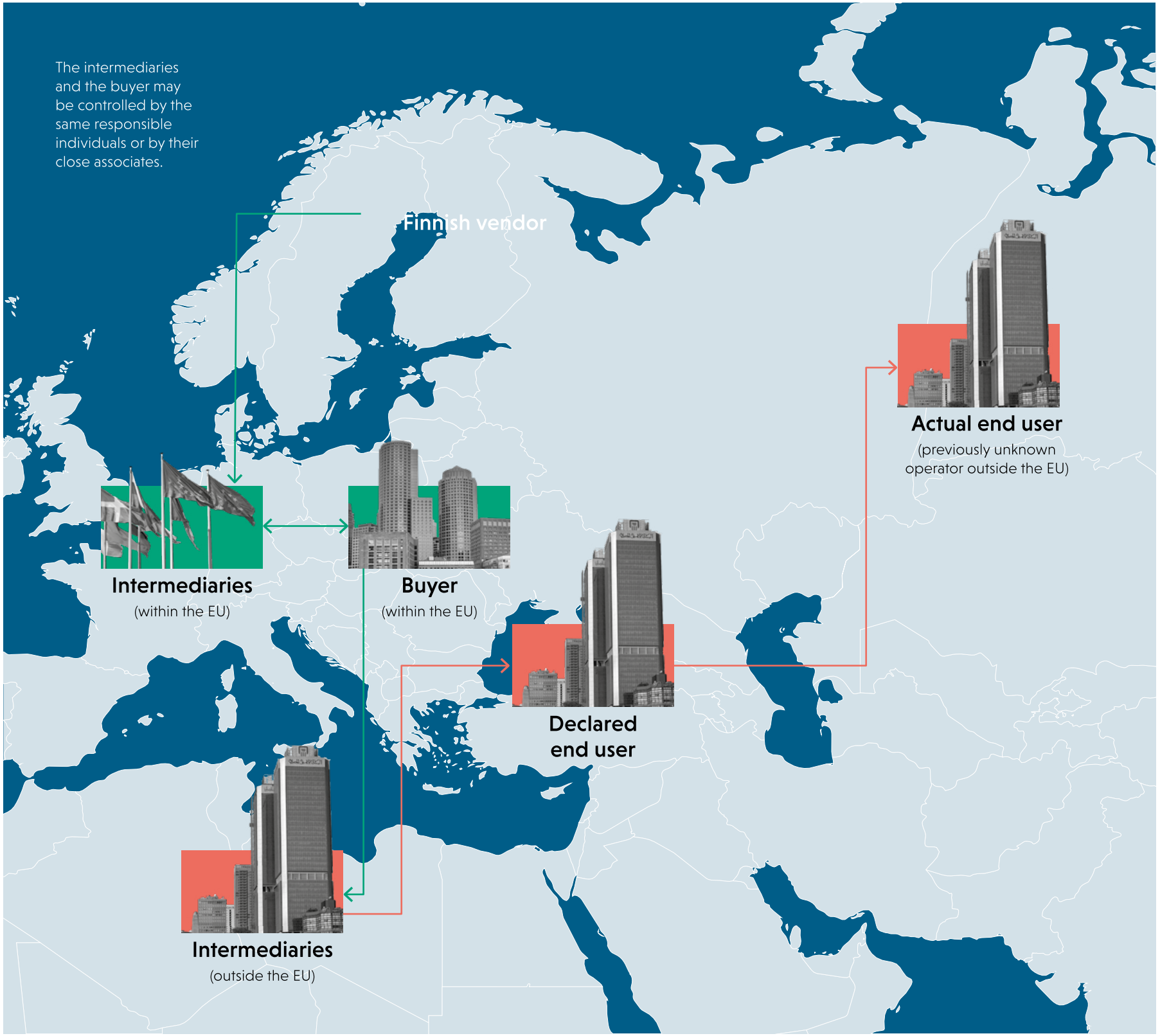
Enterprises are required to know the parties with whom they transact business. They are ultimately responsible for verifying the final destination of the products that they sell.

All enterprises and private operators should be aware of the risks involved in circumventing

Russia evades sanctions to wage war

The European Union and other Western countries have imposed sanctions in response to the Russian war of aggression. These sanctions are a foreign policy measure. One of their goals is to undermine the ability of Russia to continue its attack on Ukraine. The sanctions affect such sectors as energy, transportation, technology and defence. Recent measures have also focused on preventing sanctions-busting.

Russia has made a particular effort to evade sanctions on technology imports and energy exports, as these affect its ability to wage war in Ukraine. It will also probably continue seeking to influence the policymaking of European Union countries concerning new sanctions, and to target countermeasures against sanctions imposed by the EU and other Western countries.

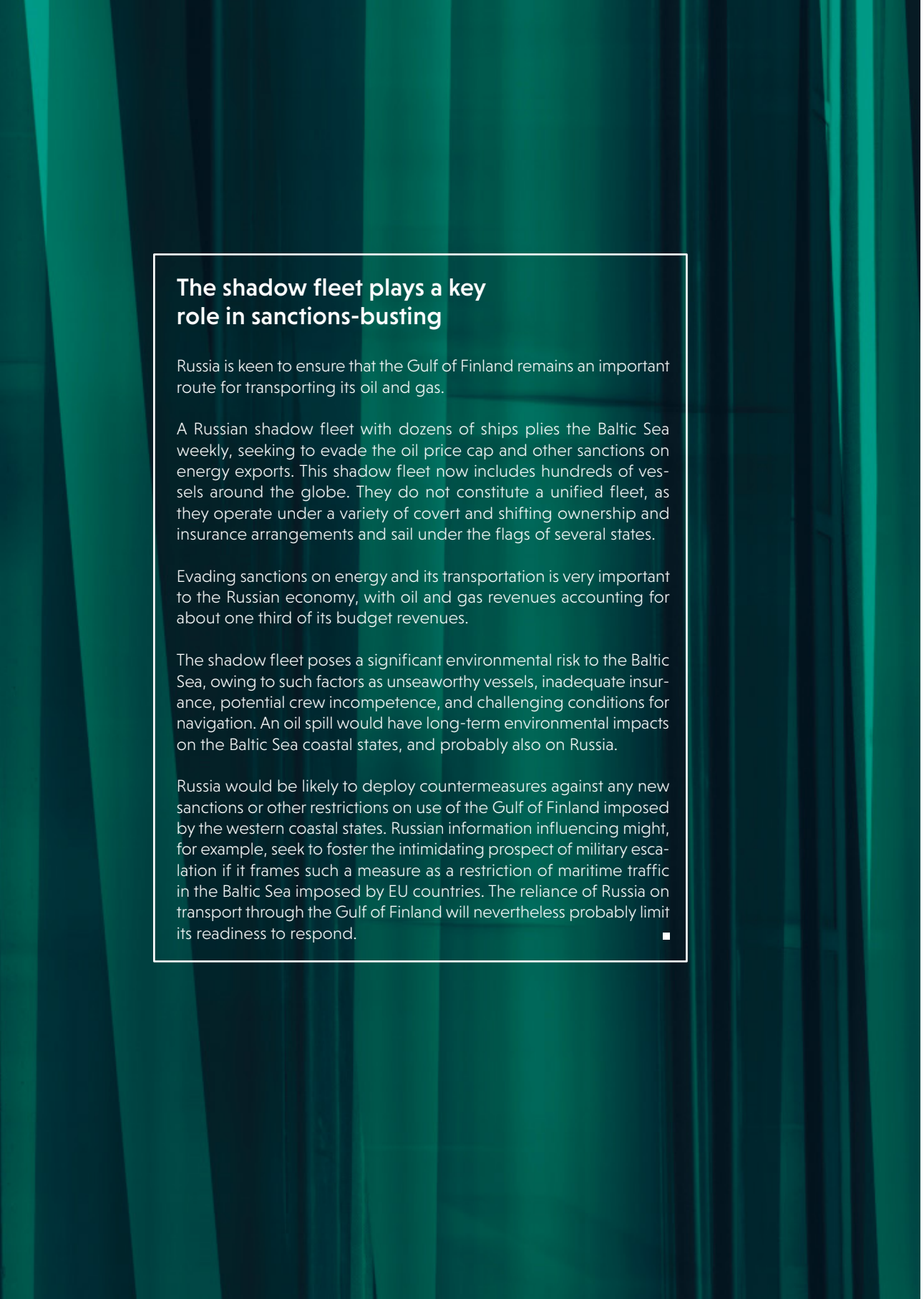


sanctions and export restrictions. Corporate management is criminally liable for complying with EU sanctions and export restrictions. Engaging in business transactions with sanctioned operators can also negatively impact a company's own business operations and its payment or financing connections.

Besides criminal penalties, involvement in sanctions-busting can cause significant reputational damage that will not necessarily always be confined to the offending business alone. This damage may also affect the stakeholders and customers of any enterprise that circumvents sanctions or export restrictions.

Businesses may contact the Customs to discuss concerns about general customs procedures and offences. The Finnish Ministry for Foreign Affairs provides advice on issues of sanctions and their interpretation, and on export restrictions governing dual-use items and the need for export permits.

Supo is responsible for working with other public authorities to ensure that controlled technology or products are not exported from or through Finland. Businesses and organisations that are the target of any suspicious approach may contact Supo using the contact form on our website. →



The shadow fleet plays a key role in sanctions-busting

Russia is keen to ensure that the Gulf of Finland remains an important route for transporting its oil and gas.

A Russian shadow fleet with dozens of ships plies the Baltic Sea weekly, seeking to evade the oil price cap and other sanctions on energy exports. This shadow fleet now includes hundreds of vessels around the globe. They do not constitute a unified fleet, as they operate under a variety of covert and shifting ownership and insurance arrangements and sail under the flags of several states.

Evading sanctions on energy and its transportation is very important to the Russian economy, with oil and gas revenues accounting for about one third of its budget revenues.

The shadow fleet poses a significant environmental risk to the Baltic Sea, owing to such factors as unseaworthy vessels, inadequate insurance, potential crew incompetence, and challenging conditions for navigation. An oil spill would have long-term environmental impacts on the Baltic Sea coastal states, and probably also on Russia.

Russia would be likely to deploy countermeasures against any new sanctions or other restrictions on use of the Gulf of Finland imposed by the western coastal states. Russian information influencing might, for example, seek to foster the intimidating prospect of military escalation if it frames such a measure as a restriction of maritime traffic in the Baltic Sea imposed by EU countries. The reliance of Russia on transport through the Gulf of Finland will nevertheless probably limit its readiness to respond. ■

Data may also be used for purposes that threaten Finland

Geopolitics and its new risks also affect data management. Information sharing increasingly needs to be assessed in the light of potential threats.

Promoting access to data gathered at public expense is an established aim in Europe, with the potential for misusing data viewed as a secondary risk or acceptable price for allowing anyone to use data in order to make nifty applications that facilitate everyday life.

The tradition of open access to data has been a cornerstone of academic research. This policy has undoubtedly served both pure and applied research very successfully.

In an evolving security context, it is nevertheless increasingly necessary to consider that data can also be used for purposes that could seriously jeopardise the security of Finland or its people.

Growth in computing capacity and advances in artificial intelligence algorithms are giving authoritarian states a major boost in their ability to exploit and combine seemingly innocuous datapools.

The need to protect communications from device manufacturer risks is already understood in Finland. We have also already responded in concrete terms to the open availability of critical infrastructure location data. We are increasingly having to reassess the sharing of other information in the light of threats that its use may pose. This is specifically a matter of risk assessment. A great deal of information may still be accessed openly without risk.

Biodata can be used to cure diseases, but also to create them

One example of open data policy concerns biodata, meaning health and genetic information. Finland operates comprehensive, well-organised registries of health data that have been fairly open to use for purposes of research, and as this is often conducted in international academic and commercial partnerships, data sharing has become commonplace.

While sharing of biodata has boosted efficiency in advancing medical science, it also enables potential misuse of that data. The risk of such misuse has greatly increased in the current geopolitical situation.

Even as China currently gathers biodata from various countries, for example, it is not sharing its own. Russia also has a long tradition in military medicine.

The most serious scenarios could see biodata misused to develop pathogens and to assess their propagation through a specific target group. By making biodata available, Finland may inadvertently assist in developing such applications. The combination of artificial intelligence and bioinformatics will boost all research, for better or worse. ■

Espionage and influencing

Overview of state espionage and influencing

The principal intelligence threat to Finland comes from Russia and China. While Russia's human intelligence activities have become more difficult in Finland, its cyber operations against Finland have grown. The intelligence interest of China in Finland is long-sustained and ongoing. Finland is also a target of intelligence interest to certain other countries, such as Iran.

Russia views Finland as an unfriendly country

Russia is the principal intelligence and influencing threat to Finland in the short and long term. The Russian intelligence services take a particular interest in how foreign and security policy is formulated in Finland with respect to such as matters as NATO policy, and also in critical infrastructure, military defence capabilities, and the defence industry. Russia applies both human and cyber intelligence methods when seeking information from Finland.

Even though influencing has always been an activity of the Russian intelligence and security services, its targets and level of activity have varied according to global political conditions. NATO members that border the Russian Federation are of particular interest to its intelligence service. As relations between Russia and the West have cooled, Russian influencing has grown more severe. Russian sabotage operations in Europe may be viewed as one aspect of this.

Russian intelligence services have applied traditional influencing methods in Finland, including information influencing or contact with policymakers and journalists. Russia uses various information influencers to reinforce narratives against Western countries and Finland, and to distort history.

Methods of influencing Russian speakers abroad include compatriot policies and the use of traditional and social media and instant messaging channels that attract a Russian speaking audience. While such efforts are not excluded in Finland, the ability of Russia to influence Finland's Russian-speaking population is limited.

Russia currently views Finland as an unfriendly country, meaning that Finnish people must be prepared for increasingly active and hostile influencing. Russia nevertheless remains a country at war whose main focus is elsewhere than Finland.

Russian cyber intelligence has increased and sharpened in Finland

Even though Russian intelligence operations targeting Finland in the cyber environment have already been highly active for years, they have recently increased and become more precisely focused. The cyber operations of Russian intelligence services against Finland mainly concentrate on state administration, and on foreign and security policy targets.

Cyber espionage is a cost-effective and replicable means of acquiring information that is independent of time or location. Russia also uses Finland as a cyber transit country, meaning that Russian intelligence services regularly use the information network infrastructure located in Finland for cyber operations that target third countries.

The risks of direct and indirect impacts of Russian cyber operations have increased. Russia actively uses cyber influencing in its war against Ukraine to disrupt and paralyse the functioning of Ukrainian society. Targeting cyber influencing in a digitalised world is nevertheless not a straightforward process, and so the unintentional targeting of cyberattacks and information operations against Finland or other third countries is increasingly likely.

The most evident phenomenon over the past year has been denial-of-service attacks against Finland and other Western countries promulgated by pro-Russian cyber-hacktivist groups. Cyber-hacktivist operations are congruent with cyber-influencing that serves Russian interests. The Russian state at least tacitly approves, or even directs such activities.

While Russia has, within certain limits, provided favourable conditions for cybercriminal and hacktivist groups for some years, the associated coordination and cooperation may have increased recently. The use of proxy actors in cyber influencing enables Russia to deny its own involvement.

Recent denial-of-service attacks may be considered to send a message that specifically targets the general public. Their primary goal is to spread mistrust and to intimidate.

Russian human intelligence has become more difficult in Finland

The Russian security and intelligence services have traditionally maintained a standing presence in Finland and other countries, with intelligence service representatives mainly operating under diplomatic cover.

The presence of Russian intelligence officers has nevertheless been significantly reduced in Finland and elsewhere in Europe due to expulsions of those operating under diplomatic cover in response to the invasion of Ukraine. Operating conditions are also hampered by travel restrictions, and by a growing unwillingness of people in Finland to have dealings with Russian operators due to the ongoing war.

The long-term threat of Russian human intelligence has nevertheless not diminished, as Russia still needs to procure information.

The change in operating conditions has forced the Russian intelligence and security services to modify their approach. While Russia increasingly seeks to employ intermediaries and to find non-diplomatic forms of concealment, these will neither substantially nor swiftly compensate for the loss of diplomatic cover. Russia is also still seeking to place intelligence officers in diplomatic positions.

Russian intelligence actors are increasingly forced to operate from bases on Russian soil. Intelligence gathering may target Finnish residents who travel to Russia or spend any time there, and may also involve the use of inappropriate methods.

Finland is a target of Chinese influencing and intelligence

China has a continuous and long-term intelligence interest in Finland that is implemented through both human intelligence and cyber espionage operations. Superpower competition, growing criticism of China in the West, export restrictions and the internal situation in China all affect the targets of Chinese interest.

The Chinese intelligence services target foreign and security policy decision-making, Arctic issues, cutting-edge technology, and groups that the government of China views as a threat. NATO membership and its impact on Finland's attitude towards China have also increased interest in Finland.

Chinese influencing is global and Finland is also a target. It is implemented by several organisations that are linked to the Chinese state and its Communist Party. Chinese influencing and intelligence operations are often closely linked, with efforts also made to engage in influencing covertly.

The aims of influencing in Finland include guiding policymaking and debate concerning China in

a direction that is congruent with Chinese objectives, and avoiding any discussion of topics that are undesirable from the perspective of China. The targets of influencing include policymakers, public opinion and people of Chinese origin living in Finland.

China also practices refugee espionage in Finland, meaning that it gathers information on, monitors and seeks to control its former and current citizens who live in Finland. The targets of refugee espionage are typically individuals who represent a group that the Chinese regime views as a threat. Such individuals or their relatives living in China may be harassed by the Chinese authorities.

Chinese cyber operations focus on critical infrastructure targets and exploiting consumer network devices

China targets Finland with cyber operations and actively uses the Finnish cyber infrastructure in operations against third countries. These capabilities and targeting of these operations are now increasingly focused on Western critical infrastructure. China is seeking to create opportunities for cyber influencing against Western countries.

The growing threat of cyber influencing and intelligence targeting critical infrastructure in Western countries is increasing the threat to Finland's national security.

Chinese cyber threat actors are increasingly exploiting poorly protected and compromised consumer network devices. In the systematic intrusion into these devices and the construction of the operational infrastructure, Chinese private IT companies are also widely utilised.

This shift is driven by both a lower risk of exposure and a significantly large number of vulnerable devices. The growing number of consumer devices now connected to the Internet, and particularly the proliferation of home routers that are either unsecured or have outdated firmware currently pose a significant risk to national security.

China seeks cutting-edge expertise and technology from abroad

China is striving for global leadership in key disruptive technologies, including artificial intelligence and quantum technology. It seeks to acquire technology from abroad to support its own economic development, including through investments, other commercial partnerships and research cooperation.

China is also acquiring expertise and technology from abroad for military purposes. Several dozen universities in China have links to the Chinese armed forces, with efforts ongoing to transfer required expertise to China through academic cooperation.

The restrictions on exports of semiconductors and their manufacturing technology imposed by the USA on China have also increased the need for China to acquire information by applying intelligence methods. Finland also has a wealth of technological expertise that is of interest to China.

Finland is also an espionage target for certain other countries

Finland holds special interest not only for the intelligence services of Russia and China, but also for those of certain other countries, such as Iran. Authoritarian states often target their espionage and influencing operations at individuals who are members of the political opposition in their country of origin, or at other groups that their governments view as a threat. ■

Russia seeks to influence European countries through sabotage

Russian sabotage efforts are most often linked to its GRU military intelligence service. Their purpose is to instil fear, and to undermine Western support for Ukraine.

Several European countries have seen acts of sabotage linked to Russian intelligence over the past two years. These acts have become a form of Russian influencing in Europe. Operations have targeted major countries in Europe and a few other states.

The influencing capacity of Russia in Europe deteriorated significantly after it launched a major invasion of Ukraine in 2022. While Russia has traditionally used diplomatic cover for its intelligence operations, Western countries have expelled numerous intelligence officers from its embassies since the war began.

Russian intelligence has accordingly been forced to change its operating methods in order to adapt to these new conditions. The shift in Russia towards a war society has also become evident in its working methods outside of Ukraine.

These include more active sabotage operations that are mainly linked to the GRU Russian military intelligence service. As a branch of the Russian armed forces, the GRU is more prone to engage in direct intelligence operations than its counterpart in foreign intelligence, the civilian intelligence service (SVR). The Russian Federal Security Service (FSB) mainly operates within the borders of Russia, although it also has powers and a history of operations abroad.

Sabotage has assumed more serious forms

Russia formerly tended to use its own trained intelligence officers for foreign sabotage operations, which were infrequent, but more carefully planned and aimed at strategic targets. Examples include the attempted assassination of the Skripals in the UK and the 2014 bombing of an ammunition depot in Czechia by GRU Unit 29155.

Russia currently relies for destructive operations on intermediaries, such as criminals or others motivated by financial gain. These operators may, for example, carry out arson attacks at even quite minimal cost without ever knowing the true identity of their ultimate client. Such proxies are typically recruited through social media and are not particularly professional.

The attacks are aimed at simple and readily accessible targets that are of symbolic or secondary importance in terms of actual support for Ukraine, such as shopping centres or other less well-protected sites. One potential target is military support for Ukraine, including its manufacture, transportation or storage.

Russian sabotage operations in Europe have nevertheless assumed increasingly dangerous forms that show indifference even to innocent bystander victims, as evidenced in news reports released in 2024 by the German and British authorities concerning incendiary devices in haulage parcels.

Russia seeks to engender fear

Russia is hoping that sabotage operations will influence opinions and the general sense of public safety, while imposing a burden on public authorities. The chosen targets have little strategic significance as such. Isolated acts of sabotage targeting military support would not significantly affect conditions on the front line in Ukraine.

The intended impact is more psychological. Russia is seeking to create a sense of insecurity with a view to influencing decisions in Western countries. As the GRU is behind the operation, it also has military objectives.

The main aim is to turn public opinion in the West against supporting Ukraine. Russia is also seeking to demonstrate its ability to act in the West, and to seek negotiating positions that will pay off in future. Even though the targets of these operations no longer have their former strategic significance, their impact has increased.

We may well see changes in Russian intelligence service operations in future. Russia may come up with new modes of influencing when cases of sabotage become public. It often acts opportunistically by experimenting with various approaches from which it reaps such benefits as become available.

The behaviour of Russia will also depend on shifts in relations between Russia and the West. If operating conditions for Russian intelligence in the West improve, for example, then Russia may very well once again begin to prefer more classical intelligence methods. Only in the longer term will we see whether the current sabotage operations become an established Russian way of working.

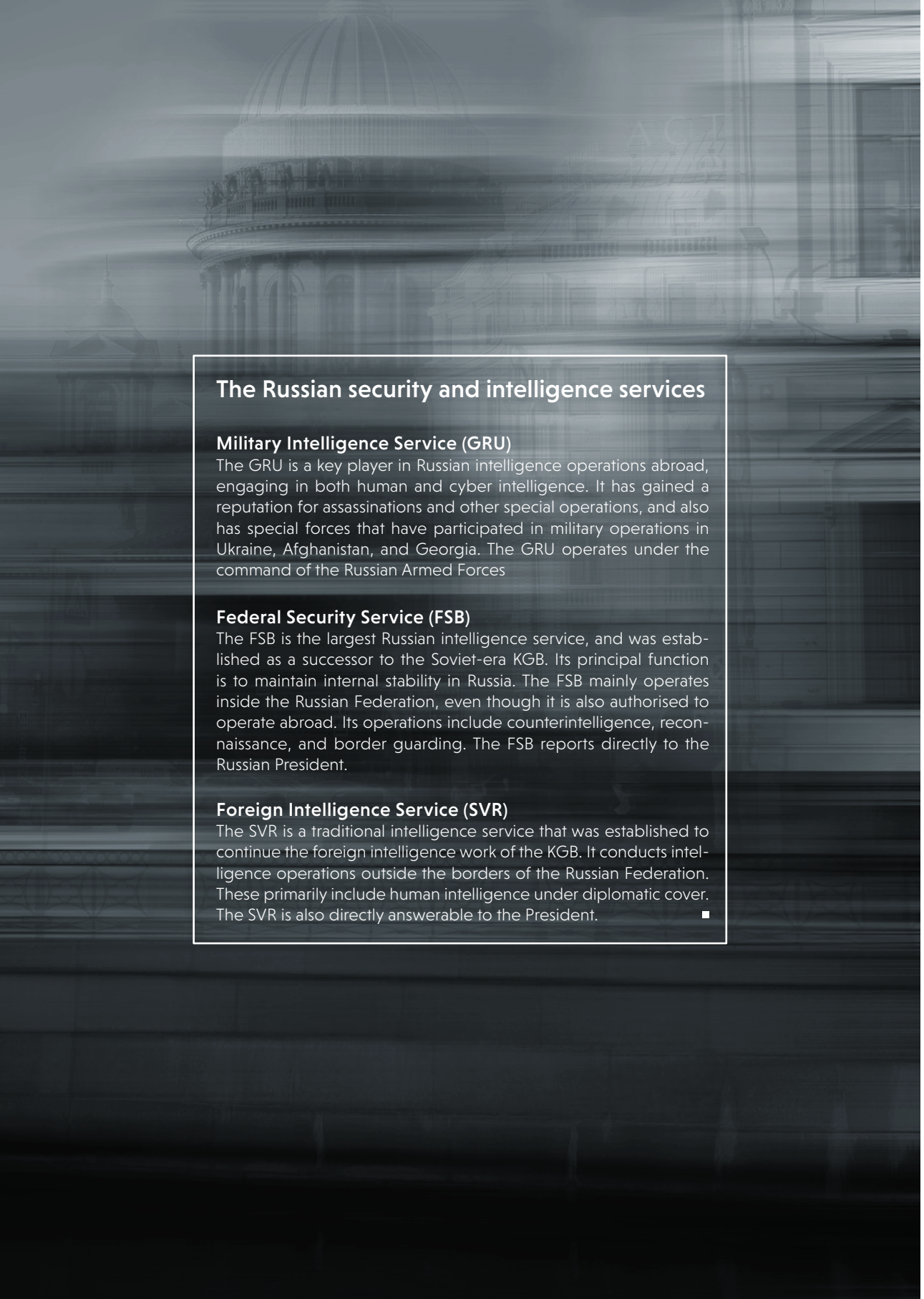
Finland is not the main target, but sabotage cannot be ruled out

Finland is probably not an especially important target for Russian operations in terms of their impact and attention value. Russia does not view Finland as a key actor that could influence policymaking on the western front.

The threat of sabotage nevertheless remains a real one that must also be taken seriously in Finland. Russia has reclassified Finland as an unfriendly country that has tightened its stance towards Russia. Supo has already included the threat of sabotage in its security assessments for some time.

The most likely targets of Russia-sponsored sabotage in Finland would also be operators that are involved in providing material support to Ukraine, such as the defense industry. Russian sabotage operations currently pose no threat to critical services.

→



The Russian security and intelligence services

Military Intelligence Service (GRU)
The GRU is a key player in Russian intelligence operations abroad, engaging in both human and cyber intelligence. It has gained a reputation for assassinations and other special operations, and also has special forces that have participated in military operations in Ukraine, Afghanistan, and Georgia. The GRU operates under the command of the Russian Armed Forces

Federal Security Service (FSB)
The FSB is the largest Russian intelligence service, and was established as a successor to the Soviet-era KGB. Its principal function is to maintain internal stability in Russia. The FSB mainly operates inside the Russian Federation, even though it is also authorised to operate abroad. Its operations include counterintelligence, reconnaissance, and border guarding. The FSB reports directly to the Russian President.

Foreign Intelligence Service (SVR)
The SVR is a traditional intelligence service that was established to continue the foreign intelligence work of the KGB. It conducts intelligence operations outside the borders of the Russian Federation. These primarily include human intelligence under diplomatic cover. The SVR is also directly answerable to the President. ■

Authoritarian state cyber ecosystems endanger international stability

National authorities need the expertise of academic institutions, private enterprise and specialists to succeed in a continually evolving cyber world. The combined capacities and capabilities of various actors in complex networks is called a cyber ecosystem. Cyber enterprises and researchers may also become integrated into the national espionage and influencing apparatus in authoritarian countries, such as Russia and China.

The cyber world has become an arena for displays of geopolitical power. States in a rapidly digitalising world have had to focus resources on defensive cyber capabilities. Strong cyber ecosystems deliver more comprehensive promotion of national security and resilience to cyber threats. Growing geopolitical tensions have nevertheless blurred the boundaries between defensive and offensive capabilities and objectives. Particularly under authoritarian regimes, cyber development has focused on harnessing national cybersecurity resources as a component of intelligence and influencing operations that serve the interests of the state. The same operational capabilities are also used for maintaining internal control in such states.

Government administrations in both Russia and China have sought to integrate the expertise of cyber enterprises and specialists into their espionage and influencing activity. This aim has been promoted through tightening legislation, investing in cyber security research, and boosting private sector involvement in producing services and tools for intelligence and influence activities. Especially China has expanded its cyber ecosystem to a particularly unprecedented scale.

What is a cyber ecosystem?

No single actor can alone defend a state in a cyber environment. Such defence requires cooperation between various sectors. Cyber ecosystems comprise enterprises involved in safeguarding the cyber environment or in service provision, intelligence and security authorities, armed forces, research institutions, the media, and other organisations that are required to protect national security in a cyber environment. Cyber ecosystems combine the resources and capabilities of these varying actors to serve the national cybersecurity of states more comprehensively.

Education and research

Public sector

Private sector

Duties

Incentives

Guidance

RUSSIA, CHINA
Detailed legislation
Laws, statutes and technological standards guide cybersecurity research, information management and training, service, software and hardware development, and cross-border data communications.

CHINA
Restriction of information sharing
Public and especially international sharing of cybersecurity information is restricted by such means as restricting free expression and preventing cyber specialists from participating in international information security events.

CHINA
Compulsory reporting of vulnerabilities
Enterprises, security researchers, specialists and even private individuals are required to report all software and hardware vulnerabilities to state authorities immediately. This duty of notification is also subject to the ban on free expression and restrictions on corrective measures.

RUSSIA, CHINA
Duty to disclose information and grant access to public authorities
Hardware manufacturers and service providers operating in China are required to assist the intelligence authorities upon request, including by disclosing information, granting access and lending infrastructure.

RUSSIA, CHINA
Financing
The government finances national security vulnerability and cyber warfare research.

CHINA, PARTLY RUSSIA
Subcontracting
Freelance actors provide independent cyber espionage and intrusion as a service.

CHINA, PARTLY RUSSIA
Private sector involvement in intelligence
Private enterprises subcontract tools and infrastructure to Chinese intelligence services.

RUSSIA, CHINA
Training programmes
China in particular has enlarged national cybersecurity-focused training programmes and courses, together with national programmes of accreditation and certification.

RUSSIA, CHINA
Cyber events
National cybersecurity events serve as information gathering and recruitment platforms for the security and intelligence services.

CHINA
National Vulnerability Database
A National Vulnerability Database gives the intelligence agencies continuous access to the latest attack vectors.

RUSSIA, CHINA
Authoritarian governance
The work of government departments that focus on industry, information technology and national security, and of their subordinate organs and associations, is strongly subject to the supreme state leadership.

CHINA, PARTLY RUSSIA
Businesses as cover for public authorities
Chinese intelligence agencies use enterprises masquerading as information security vendors as cover in cyber espionage work.

Analysis

Russia views cyber dimension as an arena for modern conflicts

The Russian cyber ecosystem combines traditional propaganda and modern technology.

Russia has a bifurcated attitude towards the cyber environment. On the one hand, it views cyber environment as an influencing platform that could endanger the internal stability, culture, values and national identity of the Russian state, and accordingly seeks to reduce its dependence on Western technology. Russia seeks not only to limit access by its citizens to the free Internet, but also to limit the ability of Western countries to spy on or influence Russian systems. On the other hand, Russia also uses the cyber environment actively as an instrument for achieving state interests and nurtures Russian cybercrime directed at foreign targets.

Russia views the information environment as an arena for conflict. This notion has guided Russia in systematically arranging its own cyber ecosystem, so that the surrounding society supports state cyber activities. At the core of the Russian cyber ecosystem are the supreme state leadership and the security and intelligence services, which are responsible for strategic planning, prioritising, and deployment of national cyber resources. Russia has managed to build a system which combines traditional propaganda and modern technology.

A flexible cyber ecosystem has been tested in practice

Russia has developed its cyber ecosystem in multiple fields. It has made an effort to train cybersecurity specialists, both at universities and in the in-house training programmes of its security authorities. Academic institutions have also supported Russia's cyber activities through expertise and development efforts.

Russia has also invested in its national cybersecurity, information, communications and technology sectors, and enacted legislation to reinforce its ability to exploit information held by private sector entities in intelligence and influencing activities. The national and state-sponsored media organisations disseminate narratives that align with Russian interests. Strictly regulated national technology and communication platforms also provide opportunities for monitoring and controlling information flows.

The combination of these varying capabilities has made the Russian cyber ecosystem a versatile entity for national security authorities to use, both in military operations against Ukraine and in cyber influencing and espionage against Western countries. Besides intelligence on foreign and security policy, Russia has used cyber operations to secure intelligence that has subsequently been used as a resource for influencing.

The Russian intelligence authorities have also conducted numerous cyber sabotage operations, seeking to disrupt the functioning of Ukrainian society. Common to these operations has been the incitement of fear, uncertainty, and mistrust, thus compromising national and international unity in countries and various alliances that are classified as "unfriendly" from the perspective of Russia.

Russia seeks to disengage from the Western Internet

Russia views continued control of information as a crucial element in maintaining its digital sovereignty. The administration feels that the national information space should be protected from external influencing. While Russia has officially embraced the goal of combating hostile foreign activity and promoting Russian culture and values, free access to information is also considered as a significant threat to the current regime.

Russia has made efforts to prevent ordinary citizens from accessing Western news websites, while also blocking Western users from accessing the websites of several Russian public authorities. Russia has also made a determined effort to disengage from the design principles of Western information networks, such as securely implemented encryption systems.

As part of its goal to bring the Internet under broader state control, Russia has also been engaged in long-term development of national alternatives for telecommunication networks, data storage and communication systems. By replacing foreign services, applications and technology with domestic solutions, Russia seeks to control the part of the Internet that is physically located within its borders or otherwise under Russian jurisdiction.

Russia intentionally enables cybercrime

Russia has for years also provided favourable conditions for criminal cyber activity on the condition that such operations are targeted outside of Russia and do not conflict with Russian national or foreign policy interests. Cybercriminals' operating methods have included ransomware attacks, with Finland also chosen as a target.

With rising geopolitical tensions, this symbiotic relationship between the regime and cybercriminal or hacktivist groups has assumed new forms, particularly after the Russian invasion of Ukraine. Denial-of-service attacks conducted by pro-Russian hacktivists have regularly targeted Western countries – including Finland. Growing hacktivism and cybercrime align with Russia's interests to undermine the trust of Western citizens in societal functions, even when such operations are not directed by state actors. Influencing through proxies allows Russia to deny its own involvement.

Analysis

China seeks cyber superpower status

China's exceptionally large cyber ecosystem poses a significant challenge to Western countries.

The Chinese cyber ecosystem is characterised by its exceptional scale. China has developed its cyber operational capabilities to a level at which its cyber resources are many times greater than those of most Western countries. This is the outcome of long-term work that has been ongoing for a decade, harnessing the Chinese information technology and cybersecurity sectors to maximise state cyber capabilities through centralised control and legislation.

The ambition to achieve technological superpower status has served as a goal for developing the Chinese cyber ecosystem. China applies its operational capabilities as an instrument of political and economic influencing and intelligence gathering, and of internal and external control. Economic influencing enables China to improve its own conditions for cyber operations abroad, while also enhancing its ability to apply economic influence through cyber operations.

The scale of Chinese cyber espionage has grown significantly in recent times, leading to large-scale theft of politically and economically important information. Chinese cyber operations evolve continually, using increasingly advanced methods. State cyber operations no longer focus solely on information gathering, but actively seek to create opportunities for cyber influencing by such means as penetrating Western critical infrastructure.

Chinese cyber ecosystem investments have fundamentally reshaped the field of cybersecurity, and now pose a significant threat to the national security and stability of Finland and other Western countries. Western countries are facing an increasingly complex challenge in which China is able to make extensive and flexible use of all resources in the cybersecurity sector to achieve its economic, political and military objectives.

The Chinese Communist Party and intelligence agencies at the core of the cyber ecosystem

In the same way as Russia and many other countries, China has also centralised cyber regulation and coordination directly under top-level national government. This means that the Chinese Communist Party plays a significant role in guiding the cyber sector. Committees specialised in cyber governance direct national cyber strategies while seeking to align cyber norms and standards of the international community with Chinese national interests through traditional diplomacy. The state leadership can directly guide offensive cyber operations by intelligence agencies.

Laws, statutes and technological standards not only guide the principal policies of cybersecurity education, research and information management, but also require cyber organisations and individuals to support intelligence and espionage operations that serve the interests of China. In addition to all of this, Chinese public authorities apply financial incentives to guide the private sector in developing services, software, and hardware that meets the needs of intelligence operations.

Centralised control and legislation have enabled China to assemble various domestic actors into a unique cyber ecosystem around its agencies and intelligence services. For example, private sector contributes to Chinese intelligence by providing infrastructure and tooling for cyber operations.

China has also managed to create incentives for malicious cyber activity, with private contractors carrying out intrusions and cyber espionage operations independently, in line with the interests of intelligence agencies. Front companies masquerading as information security operators also play a prominent role in Chinese international cyber espionage operations.

China's cyber ecosystem could also give it an edge in any conflict, as a diverse network of cyber actors can not only swiftly generate cyber operational capabilities as the need arises, but also provide preventative or deterrent protection against anti-China activities.

China integrates the education, research and business sectors into cyber operations

The Chinese cyber ecosystem extends strongly into education and research. The state finances research by Chinese universities and research organisations into information security vulnerabilities and cyber warfare. China collects intelligence on vulnerabilities into a national vulnerability database, from which it is immediately available to security and intelligence services.

While providing generous support to students departing for foreign universities, China imposes funding conditions that require these students to return to China for a specified period after completing their studies. Simultaneously China limits opportunities for its own security researchers to attend international security events and competitions to prevent the sharing of identified vulnerabilities with a wider audience. It has instead invested heavily in national information security events arranged jointly between state institutions and private sector operators that serve as forums for mapping technological capabilities and talent.

China leverages its education sector to address the deficit of cybersecurity professionals identified in its cybersecurity strategy by increasing cybersecurity-focused education programmes. Individual Chinese universities have also directly supported the cyber espionage operations of Chinese intelligence agencies through cultivating and procuring possible targets and vulnerabilities for exploitation, and through innovation, development and expertise in cyber methods. Both national information security events and universities serve as recruitment platforms for the security and intelligence services. ■

China is using social media platforms for intelligence gathering

Remote recruitment over social media brings less risk of exposure for an intelligence actor than any face-to-face encounter. The involvement of Chinese intelligence may be hard to detect when contacts are made on social media platforms.

Chinese intelligence and influencing agencies

There are several state organisations in China that specialise in intelligence and influencing operations.

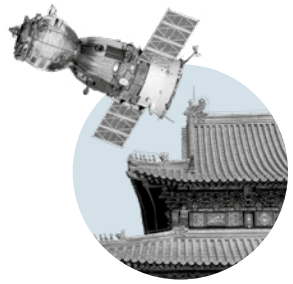
The Ministry of State Security (MSS) is a civilian intelligence service that engages in intelligence and counterintelligence operations, including human and cyber intelligence work in other countries.

The Chinese Military Intelligence Directorate (MID) is a military intelligence service.

The Chinese Ministry of Public Security (MPS) is primarily responsible for policing, criminal investigations, counter-terrorism, border control and immigration, but also discharges counterintelligence and foreign operations.

While maintaining the party's relations with political parties abroad, the **International Department of the Communist Party of China (IDCPC)** also gathers information on political conditions elsewhere and seeks to convey a favourable impression of China to policymakers in other countries.

The United Front Work Department (UFWD) is another organ of the Communist Party of China with principal responsibility for coordinating united front work. This work seeks to promote the interests of the Chinese Communist Party both in China and elsewhere, including by involving Chinese expatriates in advocacy work that serves the party's interests.



The Chinese intelligence services are actively using LinkedIn and other social media platforms to recruit sources of human intelligence. People in Finland are also targets of interest for Chinese intelligence.

Social media platforms provide a cheap and effective means for the Chinese intelligence services to recruit or seek out human intelligence sources. Selecting and approaching suitable targets is easy on LinkedIn and similar platforms.

Intelligence actors using social media platforms have less risk of exposure than those engaging in face-to-face human intelligence, as they can do so without leaving their home country. Verifying the involvement of Chinese intelligence in contacts may be difficult, especially in the early stages.

Besides recruitment operations, intelligence services actively gather information from social media platforms for various purposes.

Approaches are hard to recognise

The recruitment process on LinkedIn typically begins when an intelligence officer or their agent approaches the target individual on behalf of some business enterprise. This may involve asking the target to write a report or provide consultation on some topic of interest to China, such as policymaking or cutting-edge technological expertise.

The person requesting the service will not necessarily have any evident direct connection to China. For example, they may pose as a representative of some real or fictitious recruiting or consulting agency that seems unrelated to China.

The information initially requested is often available from public sources, and some fee may also be payable for complying with the request. Targets who comply may be asked to provide more confidential details at a later time, or they may be lured into travelling to China.

Efforts will be made at some point to transfer contact to a professional intelligence officer if the target was initially approached by an agent.

Always advise Supo of suspicious approaches

Intelligence gathering and recruitment efforts through LinkedIn and similar platforms have become an established practice of the Chinese intelligence services, and it is wise to be wary of unusual and unexpected approaches. These should be reported in the first instance to the department that is responsible for security in your own organisation.

You may also contact Supo on suspecting an attempt at recruiting. This is worthwhile even if the potential recruitment process has already progressed further.

There is every prospect that the Chinese intelligence services will continue using social media platforms. They will probably seek to make these operations more sophisticated by obfuscating their links to China, perhaps by disguising them as a regular professional recruitment process, for example. Artificial intelligence will also provide new opportunities to enhance this activity.

Contacts that increasingly request sensitive information or that extend invitations to visit China may be linked to the Chinese intelligence services. ■

Terrorism

National Terrorism Threat Assessment 2025

Supo has introduced a new five-point terrorism threat level scale. The threat of far-right and radical Islamist terrorism is at level three (elevated) on the new five-point scale. The most likely threat of a terrorist attack continues to come from lone actors or small groups advocating far-right or radical Islamist ideology.

The threat of far-right and radical Islamist terrorism is at level three (elevated) on the new five-point scale. This represents a slight increase compared to the previous threat level. In recent years, several trends have been observed in the Finnish security environment that increase the threat of terrorism.

The most likely threat of attack continues to come from lone actors or small groups advocating far-right or radical Islamist ideology. There are individuals in Finland with the motivation and capacity to mount a terrorist attack. The threat of other terrorism is minimal.

Terrorist attacks in Western countries are also likely to inspire such incidents in Finland. Extremist propaganda internationally stresses individual population groups, such as ethnic, religious and sexual minorities, together with public authorities and policymakers. The terrorism threat level in Finland is also affected by an escalation of conflict in the Middle East that has activated representatives of various extremist ideologies in Europe.

Online radicalisation of young adults and minors is a key international trend. This is also visible in Finland, both in radical Islamist and far-right contexts. Radicalisation of young adults and minors will probably be reflected in the near future also among individuals who are targets of counterterrorism work. A growing general interest in violence has been observed in the radicalisation of young adults and minors, which is also noticeably occurring at an accelerating pace.

Networks are crucial to far-right activity

The number of far-right counterterrorism target individuals in Finland has grown in the 2020s. While primarily interested in firearms and explosives, far-right terrorists also use simple improvised means, such as bladed weapons. Their most likely targets are ethnic, religious and sexual minorities, together with parties who are viewed as ideological opponents, such as politicians or public authorities.

While the organised far-right movement poses no direct terrorist threat in Finland, it can serve as a platform for radicalising individuals and small groups, and for ideologically motivated violence. Some right-wing extremists in Finland have shown interest in acquiring firearms and explosives, and in learning how to use them. This interest in weaponry arises partly from an idea of preparing for a collapse of society that the ideology envisages.

Far-right counterterrorism target individuals are typically young males with an interest in violence, of whom some have problems of mental health and life management. Far-right rhetoric stresses the threats experienced by the white population, preparation for social instability and warlike conditions, inspiration drawn from attacks that have gained prominent media visibility, and the glorification of terrorism online.

The internet is crucial to far-right activity. Some Finnish people, including minors, actively participate in discussions that glorify violence. Several plotted attacks, both in Finland and internationally, have been linked to an online Siege culture that advocates the use of political violence to overthrow the present social system.

International trends amplify the threat of radical Islamist terrorism in Finland

The most likely radical Islamist terrorist attack will be mounted in a public place using unsophisticated instruments. International radical Islamist propaganda calls for violence, especially against parties that are understood as hostile to Islam. These targets represent Christianity, Israel, Judaism, and sexual minorities. While terrorist organisations in conflict areas are still seeking to mount and promote attacks in Western countries, a large-scale attack in Finland remains unlikely.

Radical Islamist activities in Finland still focus mainly on supporting international terrorism by such means as producing and disseminating propaganda, raising funds and enlarging support networks. Some international trends that also increase the threat of radical Islamist terrorism to Finland and

Why change the terrorist threat level scale?

Supo applied a four-point scale when monitoring the terrorist threat level in 2017–2024. The five-point scale was introduced in 2025. The threat level scale assesses and communicates the threat of a terrorist attack in Finland, or against Finnish interests abroad. The national terrorism threat level is determined according to the greatest threat.

A five-point scale is more flexible than a four-point scale for assessing and communicating a threat.

"Several trends in the Finnish security context have amplified the threat of terrorism in recent years. This explains why the threat now reaches level 3 (elevated) on the new five-point scale. It is important for us to be able to describe such an increased threat more precisely," explains Supo senior analyst **Anna Santaholma**.

The other Nordic countries also use a five-point system to assess the terrorist threat level.

Supo continally reviews the threat level, releasing its threat assessment at least annually.

Finnish interests have emerged over the last two years.

Desecration of the Quran, and especially expanded conflicts in the Middle East have served as radicalising and mobilising factors in the European radical Islamist context. The changes have been reflected in such outcomes as an increase in terrorist attacks and aborted attack plots.

Networks of the Islamic State (ISIL) terrorist organisation and its Afghan province (ISKP) have become more active in Europe and neighbouring regions. Radical Islamists of Central Asian and Caucasian origin are particularly highlighted in the international activities of this group.

The Finnish National Bureau of Investigation (NBI) launched an ISIL-related preliminary investigation last autumn into participation in the activities of a terrorist group. NBI managed to track down these suspects thanks to intelligence gathered by Supo, which has continued providing specialist support to the investigation.

ISIL, al-Qaeda and the groups that swear allegiance to them continue to pose the most important terrorist threat globally. These organisations have exploited symbolically significant events in their propaganda, making increased calls for attacks on Western countries. The threat posed by terrorist organisations mainly focuses on unstable regions of Africa, the Middle East and South Asia, to which these organisations also seek to attract foreign fighters.

ISIL has continued its terrorist operations in the conflict zone of Iraq and Syria, and has sought to inspire, support and mount terrorist attacks in Europe. The ascent of the radical Islamist Hayat Tahrir al-Sham (HTS) to power in Syria and the instability that this has caused will probably give ISIL greater freedom to operate in the region. The broader impact of the change in Syria and beyond will only become apparent over a longer period.

One individual who left Finland for the conflict zone in Syria and Iraq returned in 2024. There are still about 50 people from Finland in the conflict zone, and while most have probably now perished, these deaths have not been confirmed due to the conditions prevailing in the region.

The threat of other terrorism is minimal

The threat to Finland from other forms of terrorism remains low. The activities of the far-left in Finland are mainly non-violent, focusing on supporting Kurdish activists and radical anti-fascism. Some individuals on the far left nevertheless remain ready for violent action. Violence is particularly evident in clashes with far-right demonstrators. The Finnish operations of the Kurdistan Workers' Party (PKK) terrorist organisation mainly focus on support work.

Far-left attacks in other European countries have targeted businesses and the public sector. While sabotage of infrastructure is a typical measure of far-left terrorism, violence also occurs at demonstrations, and is primarily targeted at perceived enemies, such as political opponents and public authorities. ■

Radicalisation of minors has become a persistent problem in Europe

Radicalising of children and young adults is a feature of both radical Islamist and far-right terrorism that can also be seen in Finland.

A fascination of minors with violent extremism and participation in terrorist activity has been a growing trend in Europe in recent years. Participation has increased among young adult supporters of both radical Islamist and far-right ideologies.

The Internet plays a key role in radicalising minors of all ideologies. Minors typically participate by producing, translating, and distributing radical materials.

Participation in violent activities is also increasingly common. The authorities in Europe have disrupted several suspected terrorist attack plots involving minors in recent years, with one radical Islamist attack also committed by a minor in Europe last year.

Several European countries have expressed concern about the radicalisation of children and young adults. This phenomenon has evidently become a longer-term trend that also affects Finland. Even though its main focus in Finland remains young adults, extremist ideas have also been found to appeal to minors, with a rising number of observations of this phenomenon noted in recent years.

Public authorities must work together to combat radicalisation of children and young adults. Supo has arranged training on this topic for education sector staff in municipalities, for example.

Online communities are a key factor

Social media platforms have made radical ideologies and the actors and communities that represent them accessible to young people more readily and with fewer risks. Virtual communities provide an important peer group for people who support or are interested in extremist ideologies, enabling them to reinforce their views and gain acceptance for them.

These activities rely on closed messaging applications and discussion platforms that may be used to spread propaganda, and to incite or direct attacks. Members of smaller breakaway groups from larger communities may also be urged or encouraged to engage in operations outside the virtual environment.

While both radical Islamist and far-right online communities are typically international, there are also communities that are more local, or that bring together speakers of particular languages. Finnish young people also participate in these communities.

These networks are usually not the sole cause of radicalisation. There are many underlying predisposing factors. The sense of belonging provided by online communities and groups can nevertheless play a significant role in radicalisation. Users may turn to them for social approval or a sense of significance.

The growing importance of online activity has been found to accelerate individual radicalisation, with readiness for violent action developing more swiftly in cases that give the greatest cause for concern.

Children and young adults who have been exposed to extremist thinking in their immediate surroundings form a special case. These individuals are more susceptible than average to radicalisation. Intergenerational radicalisation also occurs in Finland within the settings of both far-right and radical Islamist activity.

Propaganda exploits popular culture

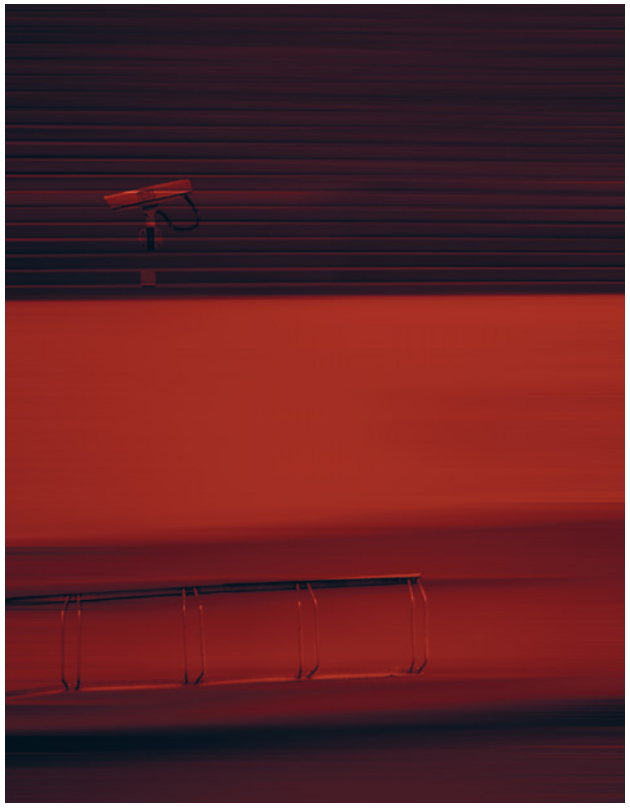
While radical actors do target propaganda at children and young adults, minors can also actively produce content for one another and for adults. Children in radical online communities may also pretend to be older and adopt roles that are similar to adults.

The producers of propaganda draw content from games and popular culture that are favoured by young people. Short videos, memes, and gamified content are skilfully employed nowadays in both radical Islamist and far-right propaganda. Lone independent actors have become increasingly important sources of propaganda in recent years.

Worldviews are often individually constructed by combining ideas from various ideologies. ■

Growth in reports concerning the radical far right in security clearance vetting

While there are many underlying reasons for the increase in reports, there are no clear indications that far-right actors are systematically gravitating towards certain sectors.



The number of security clearance vetting investigations conducted by Supo has increased significantly. While just under 70,000 investigations were completed in 2019, this figure already exceeded one hundred thousand for the first time in 2024.

The number of reports in recent years related to organised or terrorist-linked far-right groups, such as the Nordic Resistance Movement that was officially disbanded by court order, has clearly grown in Supo vetting investigations. A sixfold increase in the number of reports has been recorded since 2019. While this growth does not directly indicate any increase in far-right activity, this is one potential cause. An increase in resources devoted to oversight is also an underlying factor.

For several years, the Supo counter-terrorism threat assessment has identified radical Islamism and the far right as the most significant terrorist threats to Finland. Extremism is classified at varying levels of severity, of which terrorist activity is the most serious and rarest form.

The most likely threat of a terrorist attack comes from lone actors and small groups. Organised right-wing extremism may serve as a platform for radicalising individuals and small groups, increasing the threat of violent action from this source.

Far-right links detected in security vetting vary in strength. A growing number of these reports are relatively new. Most serious observations concern organised right-wing extremism or right-wing terrorism. The most serious cases relate to individuals with strong ties to organised right-wing extremism, who are seeking access to some security-critical position or organisation.

The far right has not systematically targeted particular sectors

Supo has not noted any more widespread propensity of individuals with far-right connections to approach particular employers or positions. More reports are received concerning larger organisations, as more security clearance vetting investigations are conducted for them. Most reports are made in security clearance vetting for the construction and IT sectors.

Some 2-4 per cent of security clearance vetting investigations disclose details that should be notified to an employer. Supo sends a written notice to the employer in such instances.

The most common written notices concern references to police records or financial difficulties. These account for about 90 per cent of cases. While reports related to the far right do not form a large proportion of all details notified to employers, the number of such reports has grown.

Supo always exercises individual discretion when deciding whether it is essential to notify a potential employer of some detail. This means that employers are not automatically notified of all reports. ■

Security clearance vetting is an assessment of reliability

Security clearance vetting investigations play an important role in preventative security work. These investigations seek to prevent foreign powers, extremists and other hostile actors from accessing details of importance to Finland's security.

Security clearance vetting examines factors that could render a person vulnerable to influence or pressure, or that could affect their reliability in some particular capacity.

In each individual case and in relation to the duties in question, Supo considers whether it is necessary to notify the employer of details disclosed in the investigation. For example, serious financial difficulties could expose an individual to attempted influencing.

Employers are in no way bound by the findings of security clearance vetting, and always draw their own conclusions as to whether the details notified by Supo will affect recruitment or other measures.

The year at Supo

The Finnish Security and Intelligence Service (Supo) reports to top-level national government on unique and proactive intelligence that it has gathered and analysed concerning national security threats. Supo also combats terrorism, prevents espionage, and conducts security clearance vetting.

National security must be protected around the clock on every day of the year. Over 580 Supo staff members do this work in offices, in the field and online – throughout Finland and also abroad. In this annual digest, six Supo employees share some thoughts on their busy working year.

Ilkka Hanski, Head of Vetting: "We have worked to improve the quality of vetting"

With a significant rise in the number of investigations, this has been another busy year for the Vetting Department. Long-sustained growth finally saw the number of investigations exceed one hundred thousand for the first time this year, with a total of some 115,000 investigations completed.

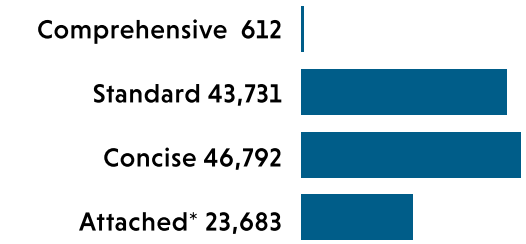
While this growth has been affected by new legislation in recent years, Supo has also consistently worked to enlarge the scope of vetting to include all key operators. Discussions have been held with organisations that are already involved in the vetting procedure to ensure that all correct functions are also security vetted.

We have also worked to improve the quality of vetting. Standard vetting procedures increasingly involve investigating foreign interests. A greater number of personal interviews are also conducted.

The average duration of the vetting procedure has shortened as we improve our processes, reducing the threshold at which organisations decide to use vetting. The impact of our work is evident in a client satisfaction score of 95 per cent achieved in a survey conducted last year. Some 97 per cent of our clients considered vetting important for their organisations.

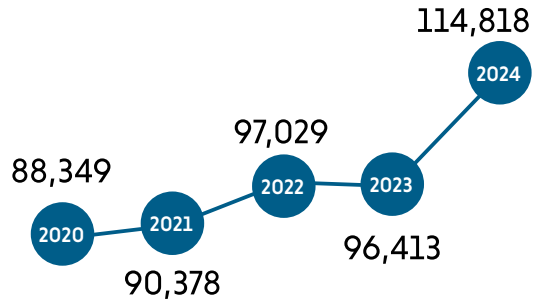
The Supo Vetting Department also issues opinions on residence permits, naturalisation and visa applications. The number of such opinions has also grown. They enable us to help ensure that individuals who jeopardise national security do not enter Finland.

Security clearances 2024



*A new vetting is not always needed when an individual's duties change.

Security clearances in total



A Supo staff member working in surveillance: "We are often present outdoors, where people are"

I have been working for some years in the surveillance duties that are the core of Supo intelligence gathering. Surveillance refers to covert observation of an individual or group in order to reveal important intelligence and protect national security.

Acquiring unique intelligence that is not otherwise available is the mission of Supo. Independent intelligence gathering process by Supo is essential in this regard.

We are often present outdoors, where people are. With intelligence targets seeking to operate professionally and covertly, we have to outplay them at their own game. Even though online information gathering has become increasingly important, a great deal of intelligence must still be acquired in the real world.

Our work is challenging and calls for perseverance. Intelligence gathering operations can be time-consuming, with the actual results only coming to light after some years. We also recognise that our work provides only one piece, with multiple players involved in assembling the larger jigsaw puzzle of civilian intelligence.

Our past year has also been exceptionally busy. We have applied intelligence methods in a wide range of ways, acquiring information of significance for national security.

The year has also been stressful for our staff, combining a large workload with an uncertain economic situation. Staff members have been concerned about whether we will be able to continue working in this way with diminishing finances. The presence of Supo in protecting society requires human resources.

Teemu Liikkanen, Head of Counterintelligence: "We must find new ways to combat espionage"

I took up the position of Head of Counterintelligence at the beginning of September 2024. Even though I was already expecting a challenge, I was still surprised by how busy we were, and by the sheer volume of duties and information involved.

This is a job where you deal with truly major issues and responsibilities. Matters of espionage and influencing that target Finland are not confined to Supo alone, but concern the whole country. They also make this work interesting and rewarding, especially when we succeed.

While not always glamorous, the importance of this work is never lost on us. Much like many forms of specialist work, it involves attending many meetings, and a great deal of reading, studying, and writing.

As Head of Counterintelligence, I seek to make our work increasingly proactive. Russia has traditionally engaged in human intelligence under diplomatic cover, but this has now become significantly more difficult. Our adversary has accordingly been forced to find new ways of acquiring intelligence, and we must in turn also find new ways of combating espionage. Ideally we will be able to anticipate the plans of our antagonist before they can be implemented.

Evolving conditions and complex threats mean that we must continually enhance our operations. My contribution will hopefully include helping to break down barriers and enhance cooperation between departments.

Counterintelligence is a traditional core function of Supo. Reforms must be implemented with respect for history and the preservation of aspects that are worthwhile.

Cyber intelligence officer: "Crazy-sounding solutions might just lead you in the right direction"

My job description involves gathering intelligence from various data networks. Our team serves in the manner of a corporate service specialised in applying various online information gathering and intelligence methods.

Our days vary greatly, depending on intelligence gathering needs. We may collect information about Russia on Monday, but then change the subject to counterterrorism on Tuesday. With duties covering the entire scope of Supo, I cannot say that any single theme dominated our work last year. Obviously we are continually engaged with signals from the East. This is work done to order, as the Internet never sleeps!

Open sources are an important starting point for almost all of my work. Information from open sources may be compared with intelligence gathered by other methods, or from such sources as other official registers. Open source intelligence is an excellent tool for guiding the use of intelligence methods proper. We employ certain intelligence methods in our own unit while supporting other units in their specialisms.

Our team broadly represents three types of expertise. Our police detectives are good at piecing together jigsaw puzzles, whereas we also include people who are proficient at various languages (most notably Chinese, Russian and Arabic), and naturally also IT specialists. It is unusual to find an individual who combines all of these talents.

We work closely with subject specialists, training them in using open sources. For example, an analyst who specialises in China may take a very different view of information gathered.

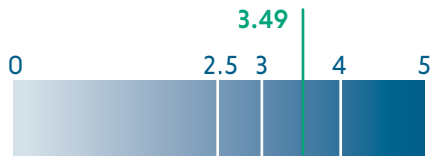
My work is characteristically quite independent, with nobody offering advice on how to approach an assignment, as a very wide range of methods may be effective. On the other hand, team support can be invaluable when you have been struggling with some problem for a long time. A colleague with a fresh perspective may well notice something that you missed. It is surprising how often a colleague comes up with some amusing, imaginative, and crazy-sounding solution to a problem that ultimately helps you get on the right track.

Intelligence work always involves various mental biases that professionals should be aware of. One well-established mental bias of online analysts is the idea that someone must have already noticed something, so it's not worth reporting on. Practical experience has nevertheless taught us that it is always worth speaking up on suspecting that you have found something that may be of interest to Supo. The best part of my job is that even the tiniest nugget of data unearthed by our team may stimulate other intelligence gathering.

Cyber intelligence can sometimes feel like looking for a needle in a haystack. Or as we put it: like trying to find a little log cabin on a map of the world. But we nearly always succeed!

Trust and reputation

A 2024 survey conducted by T-Media studied public confidence in Supo and the reputation of the organisation. The figure for reputation summarises the public evaluation of Supo's work, administration, finances, management, responsibility, image as an employer, interaction and ability to innovate.



0–2.5 Very poor
2.5–3 Poor
3–3.5 Fair
3.5–4 Good
4–5 Excellent

Head of International Affairs: "International cooperation is a key capability of Supo"

The threats that affect Finland have grown more complex in recent years, with repercussions potentially felt even from more distant crises. International exchanges and comparisons of information help us to analyse the operating models, interdependencies and trends of threat factors, and so international networks and cooperation are becoming increasingly important in our intelligence work.

International cooperation is a key capability of Supo, providing a means of exchanging unique information. For example, the intelligence that we acquire through international cooperation is an essential part of our high-quality reporting to top-level government.

It is evident from the growing volume of correspondence that Supo has engaged increasingly in international cooperation. This is part of the daily routine at Supo, and is pursued extensively in various departments.

Besides bilateral intelligence exchanges, cooperation forms part of the work with multilateral forums such as NATO, which has provided an effective addition to our international cooperation. NATO cooperation has become a stronger and more established part of the work of Supo over the current year. This cooperation with the alliance is not only an opportunity, but also an obligation, with Supo taking charge of aspects related to civilian intelligence in Finland that are its specialist field.

The diversification of non-military influencing and threats in recent years is also evident in the content of NATO cooperation.

International cooperation at Supo is typically a hectic activity that changes daily, as the variables of the security environment and of foreign and security policy do not usually adhere to precise geographical or time zone boundaries.

International correspondence

21,000

international messages
(sent and received)

Personnel

Average age 42.9

Employees in total 584

Employees with academic degree 72.6 %

Susanna Kallonen, Systems Manager: "Our ICT people face a tough job"

Working in ICT typically involves working with various stakeholders to solve difficult and complex technical and process-related problems. This is also the case for us at Supo in 2025.

While a challenging economic situation has also added further difficulties recently, we have managed to make progress in some important system development projects, including the Inter project launched with EU funding to bring about modern tools and artificial intelligence features that support data analysis in key Supo information systems.

This project seeks to boost work efficiency and improve the quality of working processes. Supo is hoping that development packages of this kind will further improve its analytical capabilities. The work is helping to transform Supo into a fully fledged intelligence service that is prepared to process growing volume of information.

We are roughly halfway through this project, which has so far largely achieved its measurable milestones and is progressing on schedule. One already completed element of the project is a work platform that enhances collaboration between analysts. We are now advancing to implement tools that apply artificial intelligence.

The extensive IT infrastructure work required for new Supo premises has also called for significant effort from the ICT team as we prepare our move to a new address in 2025. Everything must be in place to ensure that our systems work and routines can continue smoothly after the move. Also in this huge project, our people have demonstrated their excellent professionalism.

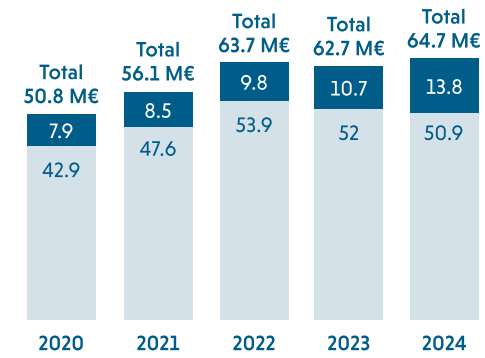
The special features of our sector also impose particular requirements when developing our information systems, adding unique complexities to the process. Our ICT people face a tough assignment in developing and maintaining numerous systems and their underlying infrastructure and hardware. These duties have been vigorously discharged with a view to matching the rapid progress of ICT development in general.

We have cause to be grateful to our highly skilled and diligent ICT staff for these successes, as they resolve these complex problems on a daily basis and help to ensure the continuity of our core operations.

■

Financing used by financial year

(million euros M€)



Realised income of the financial year

Budget financing used during the financial year (including the use of appropriations carried over from the previous year).