SUPO

National security overview 2023

Intelligence and influence operations are targeting Finland

The most active perpetrators of intelligence operations targeting Finland and its people are Russia and China. Russian intelligence is primarily interested in the security policy of Western countries, especially with respect to the Ukrainian situation and support for Ukraine, and in ways of evading sanctions. The Chinese intelligence services focus on such aspects as foreign and security policymaking and cutting-edge technology.

Russia shifts the focus of information gathering to the cyber environment

The tense security situation in Europe caused by the Russian war affects the targeting of Russian intelligence operations. Current topics of interest are the concrete consequences of Finnish NATO membership, material support for Ukraine, and ways of evading sanctions via Finland.

Operating conditions for Russia's human intelligence work in Finland have deteriorated since the war against Ukraine, and due to expulsions of diplomats. It is highly likely that Russia will have to shift the focus of its information collection to the cyber environment.

The principal objective of Russian influence operations is to undermine the unity of NATO and the European Union, and to reduce the support of Western countries for Ukraine. The accession of Finland to NATO, the continuation of the Russian war, the deepening confrontation between Western countries and Russia, and growing sanctions will probably strengthen Russian countermeasures against Finland. It is nevertheless NATO membership that will provide protection against the most violent forms of influencing.

RUSSIAN INFLUENCE OPERATIONS DISTORT REAL INFORMATION

Russia uses online platforms strategically for targeting information influencing at Western countries. It modifies the tone, details or framing of real news and information to give the content a positive spin in favour of Russia. Messaging is formulated in line with the communications culture of each media form, and cannot always be easily identified as propaganda. Russia also uses denial-of-service attacks as an instrument of information influencing.

Export restrictions imposed on China and internal conditions in China increase its need for intelligence

China is targeting human intelligence and cyber espionage operations at Finland. Chinese cyber espionage seeks information on the foreign policy views of other states and on technological R&D. Controls governing the export of semiconductors and their manufacturing technology imposed on China by the USA, for example, increase the needs of China to gather information through cyber espionage.

China has stressed that all of its people have a duty to ensure national security. Coupled with changes in Chinese legislation, this is likely to further hamper the work of many foreigners living in China, including diplomats, journalists and researchers, and will probably increase China's surveillance of people of Chinese descent living in Finland.

Threats to national security are continually evolving

Threats to national security are also changing with the digitalisation of society and technological progress. The critical services of contemporary society increasingly rely on infrastructure in space. The dual use of developing technologies, export control issues and protecting domestic R&D are emerging themes.

Cyber espionage exploits unprotected consumer devices

While most people in Finland are not targets of Russian or Chinese cyber espionage, anyone who owns an unprotected device that is connected to the network, such as a home router, can become an unwitting enabler of such operations. Consumer devices increasingly rely on an internet connection that allows them to be controlled remotely. This also provides an opportunity for unauthorised remote access by state actors seeking to penetrate the information systems of Finland or its partner countries. While things will improve with the European Union Cyber Resilience Act governing the information security requirements of new consumer devices, the impact of this regulation will not be immediate.

Unprotected home routers with outdated firmware currently pose a particularly significant risk to national security. Home router owners who fall victim to hacking are also at risk, as an intruder may use the device to impersonate the owner of the connection.

The operators manage the security settings and maintenance of devices that they supply. However, if the device is purchased privately, the responsibility for all the security aspects remains with the individual consumer.

Critical infrastructure increasingly relies on space

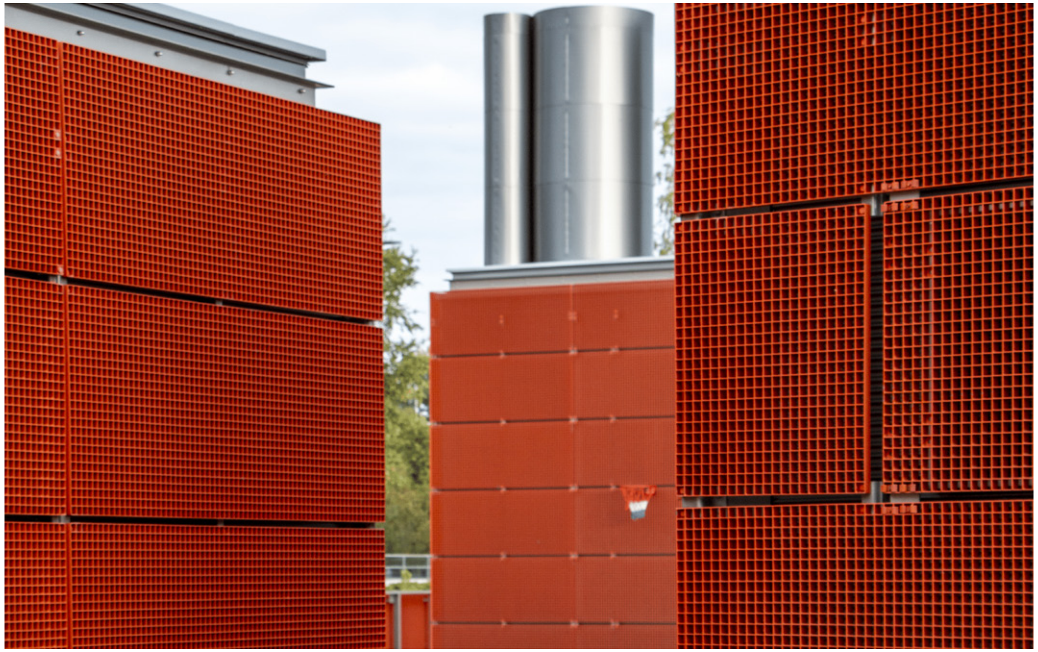
The critical services of society and certain official services require time and location information transmitted via satellites. For example, delays may arise in the work of the logistics sector when satellite location data are unavailable, and outages in satellite time data that last for weeks can affect the telecommunications infrastructure and the financial sector, for example. Society will increasingly rely on satellite services in the long term. The growing contribution of the private sector in providing services increases the associated risks when the interests of a private business or foreign power may become a factor that influences service provision during possible emergency situations.

Critical infrastructure control systems are online. These systems are usually carefully protected, and Finnish NATO membership has raised the threshold for hostile influence operations that target Finland. Most of the events that are reported in the news as cyberattacks are distributed denial-of-service (DDoS) attacks that momentarily congest a single public website without real affect to national security.

Russia is using third countries to evade export controls

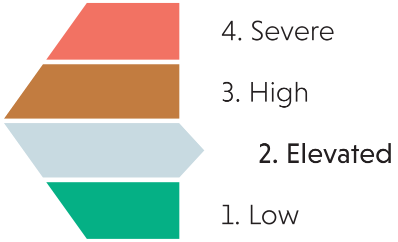
Export controls imposed by Western countries are significantly hampering the work of the Russian technology sector and industry. Russia accordingly seeks to circumvent these controls, for example by concealing details of the true end-purchaser in supply chains, and by procuring products through third countries. Russia nevertheless remains unable to replace the full range of required technology imports.

Exploitation of dual-use applications in emerging technologies and export control system loopholes is likely to increase. For example, quantum technology is generally not subject to export controls, even though it has dual-use applications, and controls are applied to exporting of certain devices or their components.



The threat of terrorism remains at level elevated

The threat of terrorism in Finland remains elevated, corresponding to level two on the four-point scale. Some 350 individuals are identified counterterrorism targets in Finland. The most likely threat of a terrorist attack comes from lone operators or small groups advocating far-right or radical Islamist ideology. Most activities linked to terrorism in Finland are support measures, such as fundraising and online dissemination of ideology.



4. Severe

3. High

2. Elevated

1. Low

Far-right terrorism involves a threat of violence

Supporters of far-right terrorism have been influenced by such elements as Siege culture, which seeks a violent collapse of the social order. These supporters view armed attacks as a key instrument for accelerating the collapse of society. They are active in online communities where extreme right-wing mass shooters are glorified, people are encouraged to mount attacks, and attack planning materials are shared.

Financing is a key form of support for radical Islamist terrorism in Finland

Terrorist financing is the transmission of collected or otherwise procured funds to persons involved in terrorist operations. Such financing is a key form of support among radical Islamist terrorism in Finland. The funds may be raised in the form of donations, for example. Efforts are often made to use legitimate business operations for laundering amounts of money that were acquired by property offences, unlawful trading and extortion of protection money. These funds are transferred to the account of an officially registered business for some reason that resembles ordinary business operations, and are then forwarded from that account to countries with less rigorous banking supervision systems or immediate terrorist activity.

The use of digital money transfers and the proliferation of virtual currencies has reinforced the informal banking and money transfer service sector. Financing of terrorist operations is an international phenomenon that crosses boundaries between economic regions. Terrorist operators can collect significant sums in a particular country without elevating the threat of terrorism in that country.

The third sector also serves as a vehicle for financing terrorism. This may involve direct transfers of funds to a terrorist operator through a nominally non-profit foundation. Funds may also be transferred to a person abroad, who then forwards them to a terrorist operator directly, via some business operation, or through the third sector.

Multi-agency cooperation plays a key role in tracking terrorist financing. Supo collaborates in this field both internationally and within Finland, with agencies such as the Finnish National Bureau of Investigation and the Finnish Customs.

SUPO

PROBABILITY TERMS USED IN THIS REPORT

Highly improbable	5 %
Improbable	20 %
Highly probable	90 %
Probable	75 %

TIME ASSESEMENTS USED IN THIS REPORT

In the near nature	0–6 months
Short term	6 months–2 years
Medium term	2–5 years
Long term	over 5 years