News and press releases

Sign up for news

Columns

National security overview

Foreign intelligence and influence operations

Terrorism

Yearbook

Brochures

Supo on social media

Media contacts

Foreign intelligence and influence operations

The most significant threat of intelligence and state-sponsored influence operations for Finland comes from Russia and China.

The main intelligence gathering method applied by the Russian intelligence services is sustained human intelligence under diplomatic cover. Western intelligence collaboration has nevertheless effectively undermined conditions for Russian human intelligence operations. Russian intelligence services have sought to exploit the cyber environment as a source of information, especially on the foreign and security policy decisions of other states, by seeking to intrude into the information systems used by target states in preparing and formulating policy.

In their home country, Russian intelligence and security services are increasingly focusing intelligence gathering operations on foreigners and their Russian contacts. Russians working in Western countries are also targets of such operations when they visit Russia.

There is clear evidence of violent acts committed by Russian intelligence in Europe. These have targeted arms depots, opponents of the regime and individuals designated as traitors by Russia. Similar attacks in Finland are improbable.

NATO membership will turn Finland into a more interesting intelligence target

Future NATO membership will make Finland a more interesting target for Russian intelligence and influence operations. One target of particular interest will be the formulation of policy in a militarily allied Finland. Russia's assessment of what kind of NATO member Finland is becoming determines the aims and methods of influence operations. Finland is portrayed as a member of a hostile alliance, whose location in the near vicinity of Russia exemplifies the threat of NATO enlargement, a narrative disseminated by the Russian regime.

Russian reactions to Finland's NATO accession process have been restrained for the time being, and Finland has not been subject to any extraordinary influencing in the course of policymaking, and of the ratification round that followed the accession announcement.

China continues to target active intelligence operations on Finland, in the form of both human intelligence and cyber espionage efforts. Examples of intelligence targets include cutting-edge technology, the Arctic region and national policymaking. The Russian invasion of Ukraine has not

significantly affected Chinese intelligence and influencing operations directed at Finland.

The power of the Chinese Communist Party is becoming increasingly deep rooted in Chinese society, increasing risks in financial and scientific operations. Technological expertise that is crucial to Chinese development but potentially subject to export controls is transferred to China through such means as corporate acquisitions and research collaboration. Dozens of universities operate in China under the auspices of the Chinese Armed Forces or of the State Administration of Science, Technology and Industry for National Defence, and these institutions also send researchers to Finland.

It is essential for risk assessments related to the acquisition of Chinese information technology to evaluate the confidentiality requirements of information that will be processed by the hardware in question. Chinese hardware manufacturers are required where necessary to assist the intelligence services of their country. The mission of these services includes cyber espionage targeting the West.

Besides Russia and China, several other authoritarian states engage in covert intelligence gathering and influence operations in Finland. These operations mainly target individuals from these countries who reside in Finland.

Critical infrastructure faces a heightened threat

The threat of intelligence gathering and influence operations to Finland's critical infrastructure has increased in both the physical and cyber environments as a result of the Russian war of aggression and Finland's NATO accession process. It is nevertheless improbable that activities seeking to paralyse infrastructure operations will occur in the foreseeable future.

Critical infrastructure operations are also affected by disruption of access to raw materials, and of global chains of production and supply. Russia's war of aggression is directly disrupting the production chains of some raw materials and processed goods. While the main impact in Finland is an increase in the prices of energy and semi-finished goods, disruptions in production chains may also affect the sustainability of critical infrastructure as the war continues.

An organisation from an authoritarian state may secure access to and influence over Finland's critical infrastructure through ownership or by providing services. There is a risk that authorities of an authoritarian state will exploit this connection to acquire information about services that are critical for society in Finland, or concerning such aspects as the operations of Finnish public authorities. Russian citizens working in critical positions in Finland may also be subject to coercion from Russian authorities.

Components for manufacturing weapons of mass destruction, such as dual-use items with both civilian and military applications, may be obtained in Finland and with the assistance of Finnish operators. Individual businesses, procurement networks, and even research collaboration are used to circumvent export controls.

Russia is seeking to bypass export controls on certain products and components. These controls may probably be evaded via third countries. It is nevertheless improbable that Russia will be able to replace previous technology imports from the West in any comprehensive way.

Assessment

Russian intelligence services will probably try to adapt their operations to respond more effectively to changed circumstances. Russia will probably focus its intelligence operations increasingly on the cyber environment. It is also probable that the threat of business espionage will grow as Russia feels the need to begin substitute manufacturing of cutting-edge technology. Russia may seek to acquire NATO-related intelligence through Finland.

Besides political policymaking, cutting-edge technology and related expertise will most probably continue as the main focus of Chinese intelligence operations.

The threat of intelligence and influencing operations targeting critical infrastructure will remain elevated in the immediate future. Disruption of production and supply chains will probably be a vulnerability in the short term.

Technology export controls imposed by the West will significantly hamper the work of the Russian technology sector and industry in the short term. Efforts to circumvent export controls will highly probably continue in Finland in the medium term.

Cyber espionage and influence operations are not the only threats in the cyber sector

Denial-of-service attacks are online demonstrations that cause access congestion in the targeted online service. Unlike ordinary demonstrations, denial-of-service attacks can be automated in ways that do not substantially consume the resources of the perpetrator. The purpose of denial-of-service attacks of Russian origin is to foster mistrust in the population of a target country concerning the functioning of the cyber environment. While denial-of-service attacks cause temporary disruption, they do not compromise data security or crash the online service. Geographically decentralising cloud services can help to defend an online service against such attacks, but this involves significant costs.

Threats to national security can be an unintended by-product of organised cybercrime. Perpetrators of online extortion may penetrate an information system to steal confidential information, and to initiate its encryption in a manner that prevents owners from accessing their information. These perpetrators then demand a ransom from the owner in return for decrypting the information and keeping it out of the public domain. Victims cannot be certain that the criminal will not sell illegally obtained information to third parties.

Probability terms used in the report

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

Time assessments used in the report

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