



National Security Overview 2020

SUPO
FINNISH SECURITY AND
INTELLIGENCE SERVICE



Phenomena falling within the field of competence of the Finnish Security and Intelligence Service (Supo) and their development are evaluated in the national security review.

Intelligence Activities Targeting Finland and Finns

Though hampered by the coronavirus pandemic in spring 2020, the intelligence operations of foreign powers targeting Finland have continued. The number of foreign intelligence personnel stationed in Finland is large in relation to the size of the country.

Several dozen foreign intelligence officers are permanently stationed in Finland, and foreign intelligence organisation staff members also engage in brief operational assignments in Finland every year.

Restrictions arising from the coronavirus pandemic hampered the activities of foreign intelligence stations in Finland in spring 2020, but human intelligence operations resumed after these restrictions were lifted. Extensive travel restrictions have made unlawful cross-border human intelligence much more difficult.

The main foreign powers engaged in intelligence operations targeting Finland and Finnish interests are Russia and China. The operations of foreign intelligence services in Finland are sustained and systematic. A sustained background interest in Finland remains, despite some variation in intelligence queries concerning current affairs. The principal goals of the operation include anticipating various political developments in Finland and influencing policymaking. Foreign intelligence services are also interested in Finnish technology and associated expertise. Finland is also still used extensively as a transit country for illegal technology exports. This particularly concerns banned exports of Western technology with military applications.

Human intelligence gathering operations have been targeting the same broad aspects of Finland's foreign and domestic policy as before the coronavirus pandemic. The targets of foreign human intelligence operations in Finland have included policy and policymaking on the Arctic, investments in Finland's critical infrastructure and other strategic areas, and the activities of Finnish political organisations.

Some specific instances have emerged of foreign powers seeking to recruit clandestine sources in Finland who can provide information that is not in the public domain. Foreign intelligence organisations also seek the assistance of individuals who can help to exert direct or indirect influence on policymaking and public opinion.

The intelligence services of some countries seek to control their current or former citizens residing or staying in Finland. Such operations reflect the efforts of intelligence services to reinforce the political system of the state that they represent, and so surveillance and harassment typically targets the political opposition or dissidents. The goal is also to recruit sources of information on target communities.

ASSESSMENT: Intelligence operations of foreign powers targeting Finland are ongoing on a large scale. The principal threat to Finland arises from the sustained operations of Russian and Chinese intelligence services in various sectors of Finnish society.

Cyber Espionage

The coronavirus pandemic has shifted the priorities of espionage to the cyber environment in some measure. Finland is a target of systematic cyber espionage operations by the same countries that show intelligence-related interest towards Finland in general, Russia and China.

Although restrictions introduced in Finland in the early stages of the coronavirus pandemic hampered unlawful human intelligence operations, new opportunities emerged at this time for foreign powers engaged in espionage to gather intelligence concerning Finland by infiltrating information systems. A substantial portion of key functions in society were relocated to remote access networks. The required scale of remote operation called for fast-track solutions in which ensuring access to information was often a key factor in data security. This also introduced new vulnerabilities for highly digitised European states such as Finland.

The countries engaged in cyber espionage targeting Finland were not immediately able to take full advantage of the emerging opportunities, as the coronavirus pandemic also affected their own operations. Where financially motivated cyber criminals can adapt more rapidly to change, state-sponsored espionage is a more systematic and managed activity that takes time to direct.

Painstaking security work will be more important than under normal conditions as the pandemic continues. Cyber espionage is currently more active than usual, and identifying security anomalies is now more challenging than in normal circumstances.

ASSESSMENT: Countries that engage in espionage are highly likely to continue active cyber spying operations as the coronavirus pandemic hampers international travel. The pandemic has also created new cyber espionage targets in the form of the pharmaceutical industry and research institutes.

Authoritarian states will probably seek to exploit the international fragmentation caused by the coronavirus pandemic, the US presidential election and Britain's secession from the European Union to engage in operations that they would otherwise be reluctant to pursue.

Painstaking security work has become increasingly important in the current climate. National security will be endangered if the need to make information accessible is prioritised over all other data security considerations when maintaining key systems.

The Threat of Terrorism in Finland

Individuals targeted in combating terrorism have significant international connections. The danger of extreme right-wing terrorism has grown in Western countries, including Finland.

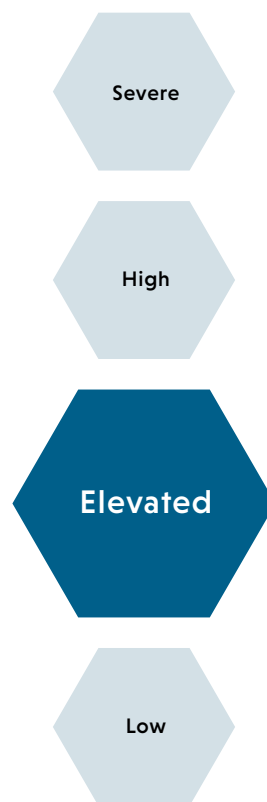
Supo has identified some 390 counter-terrorism (CT) targets. This number has remained unchanged as Supo continues to identify groups and individuals with the motivation and capacity to carry out a terrorist attack in Finland.

Significant terrorism support operations found in Finland include financing and dissemination of ideology. CT targets have significant links to foreign terrorist operators and networks. Some people have moved to Finland from conflict zones after participating in the operations of armed groups and otherwise promoting such activities in those zones.

The "Islamic State" (Isil) and al-Qaeda terrorist organisations and their supporters remain a global threat. In all probability their members and supporters are seeking to develop new tactics for mounting attacks, and will also continue to encourage attacks in Western countries.

The threat of far-right terrorism has grown in the West, with an increase in terrorist attack projects seeking to maximise casualties over the past 18 months. Supporters and sympathisers of far-right terrorist activity have also been identified in Finland. International far-right online groups and communication over social media platforms reinforce the transnational character of the extreme right.

ASSESSMENT: The likely short-term threat of terrorism in Finland remains at level two (elevated) on the four-point scale. The principal threat is posed by lone operators or small groups who support radical Islamist or far-right ideology, and are motivated by terrorist propaganda.



Threat levels are used to describe the terrorist threat against Finland and Finnish interests. The factors taken into account when assessing the threat level are the available intelligence, the operational capacity and motivation of terrorist organisations or individuals and groups linked to them, and the time span of possible attack plans.



Hybrid Influencing

Hybrid influencing is an activity of authoritarian powers in particular, that seek to promote their own interests by applying a wide range of means, usually to the detriment of the target state.

The main aim of hybrid influencing is to curtail the national sovereignty of another state. Such operations exploit the vulnerabilities of the target state, with the true agent often seeking to work clandestinely in the background.

Though it currently remains a target country, the negative impact of hybrid influencing on Finland remains minimal. Hybrid influencing includes measures taken in the political, economic,

military, information and cyber sectors. Besides any direct and immediate impact, it may also take the form of preparing for some future hybrid influencing operation.

Efforts have also been made in 2020 to exploit the coronavirus pandemic in information influencing, but the outcome of this has been minimal to date.

ASSESSMENT: State-sponsored operators remain highly willing to apply powerful means of hybrid influencing to advance their objectives. On the other hand, Western efforts to combat hybrid influencing are helping to reduce this threat.

Terms Used in the Report

PROBABILITY:

- Highly probable 90 %
- Probable 75 %
- Possible 50 %
- Improbable 20 %
- Highly improbable 5 %

TIME:

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

