SUPO

National Security Overview 2021

Summary of the overview

Intelligence and influencing operations targeting Finland

Intelligence services seek to use embedded human intelligence sources to obtain reliable and forward-looking information about Finland that is not otherwise available. Such operations are actively interested in securing insights into the preparation of major policy positions and details of state-of-the-art technology.

Cyber threats

State-sponsored cyber espionage remains the most important cyber threat. Finland is a target of continual attempts at cyber espionage, with no prospect of such operations subsiding, even in the long term.

Terrorism

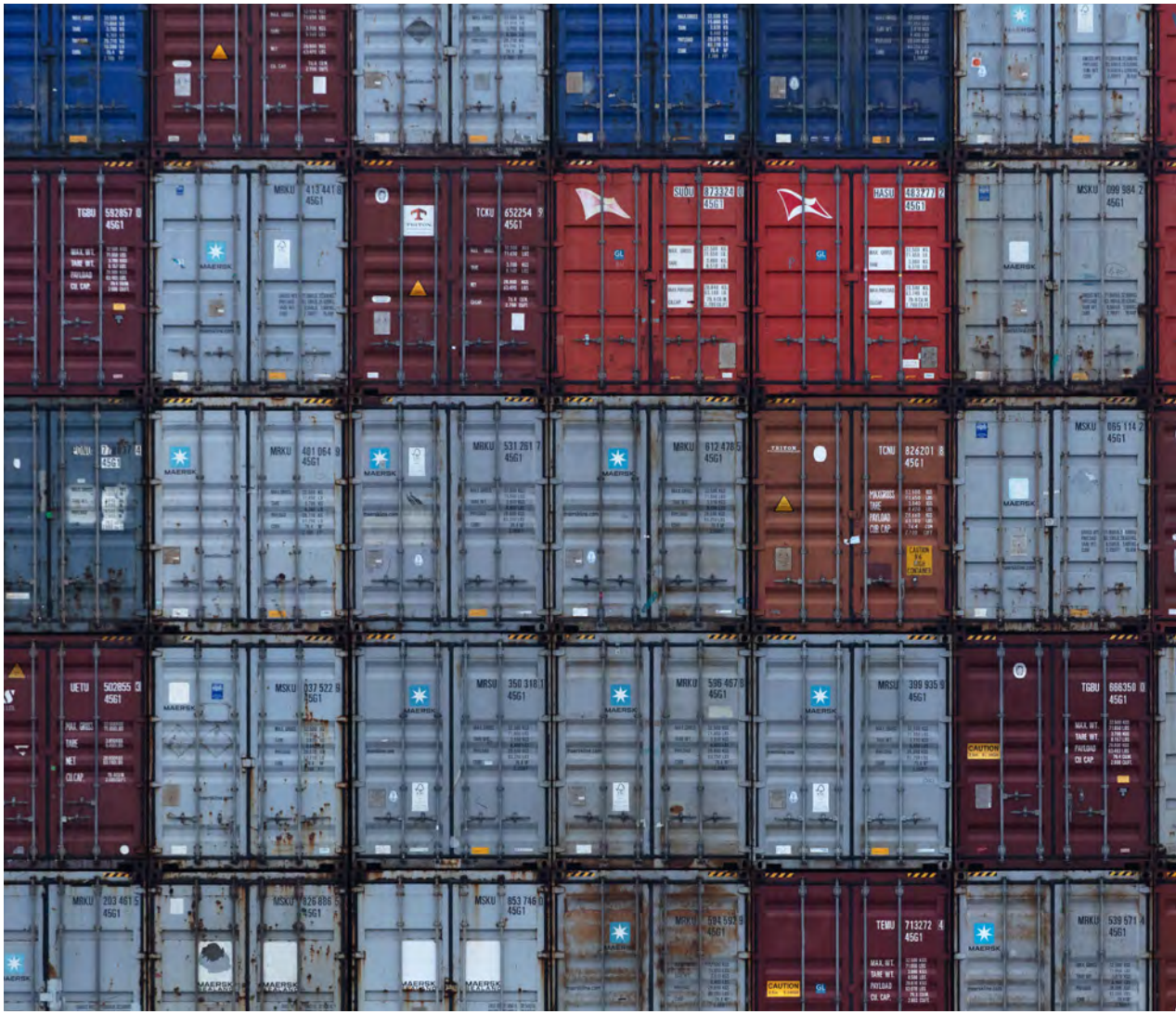
The main threat of terrorism in Finland is posed by individuals and small groups supporting far-right or radical Islamist ideologies. A significant part of their networking and other activities take place online and using communication applications.

Threats to critical infrastructure

Critical infrastructure is a long-term target of foreign intelligence operations in Finland. Authoritarian states can also access Finland's critical infrastructure through legitimate activities, such as business acquisitions and joint ventures.

Dual-use products and weapons of mass destruction

Parties seeking to procure weapons of mass destruction and components of such weaponry have directed efforts through Finland and Finnish operators. No change to Finland's role in the dual-use item supply chain is likely in the short term.



Intelligence and influencing operations targeting Finland

Finland and its population are continually subject to a broad range of unlawful intelligence operations. Finland remains a target of intelligence interest to Russia and China in particular.

Intelligence services seek to use embedded human intelligence sources to obtain reliable and forward-looking information about Finland that is not otherwise available. Such operations are actively interested in securing insights into the preparation of major policy positions and details of state-of-the-art technology. Other areas of interest include Finland's relationship with the NATO military alliance, Arctic region issues, and cyber security and expertise.

Authoritarian states covertly disseminate media and social media content in support of their domestic policies, and also seek to reshape the thinking of Finnish policymakers and diaspora communities to align with their interests.

These states also seek to promote their own economic interests by covert means.

Smaller authoritarian states also engage in covert intelligence and influencing operations in Finland. These small-scale operations mainly target individuals from these countries who reside in Finland.

ASSESSMENT

While no changes are expected in the threat posed to Finland by foreign intelligence and influencing operations, they will continue on a large scale. It is likely that the deterioration of superpower relations, growing global and regional uncertainties, and rising political tensions internationally will increase the need for authoritarian states to engage in covert intelligence gathering and influencing.

Cyber threats

Cyber threats to national security can arise in the form of cyber espionage or influence by foreign powers. The side effects of cybercrime may also pose a threat to national security as society becomes increasingly dependent on the smooth operation of information systems.

State-sponsored cyber espionage remains the most important cyber threat. Finland is a target of continual attempts at cyber espionage, with no prospect of such operations subsiding, even in the long term. Authoritarian states use espionage to gather intelligence in support of their own national policymaking, and in order to influence the policymakers who are targeted by such operations. They may also seek to exert a deterrent effect by demonstrating their capacity to operate in a cyber environment.

Cyber espionage may also seek to obtain details of R&D work with a view to enhancing the global competitive status of authoritarian states and their business operations. Information of this kind is mainly held by the private business sector in Finland, but can also be found in universities and research institutes.

The information systems that are targeted by cyber espionage may be accessed via vulnerabilities. Such vulnerabilities may also enable cyber influencing, meaning unauthorised modification of information or blocking of access to information. The damage that can be done by modifying data or preventing access to it increases as more functions of society are placed on a digital footing.

The threat of cyber influencing is currently associated with financially motivated extortion. While this is only undertaken with the prospect of financial gain, and does not seek to threaten the state of Finland, the side effects of such activities may endanger national security if they disrupt a system that is critical to the functioning of society.

The system owner is optimally placed to protect an information system, and a large share of Finland's critical infrastructure now belongs to private businesses. Ensuring business continuity remains an established part of normal corporate management, but securing information is a technical issue that is still often the responsibility of a specialised data management or security service. Outsourcing arrangements standardly manage such aspects of business continuity on a contractual basis, but measuring the effectiveness of data protection measures is not yet commonplace. This increases the risk of becoming a target of cybercrime.

ASSESSMENT

Cyber espionage is highly likely to continue, even in the long term, as global confrontation heightens the pressure on authoritarian states to procure secret intelligence from Finland with growing disregard for Finland's sovereignty.

Finnish information systems are unlikely to be targeted by the hostile cyber influencing operations of foreign powers in the medium term unless security policy conditions become significantly more difficult.

While Finland has a fairly good data security culture, it is likely that a Finnish business or branch of public administration will fall victim to a criminal ransomware attack. It is also possible for this to constitute a threat to national security.

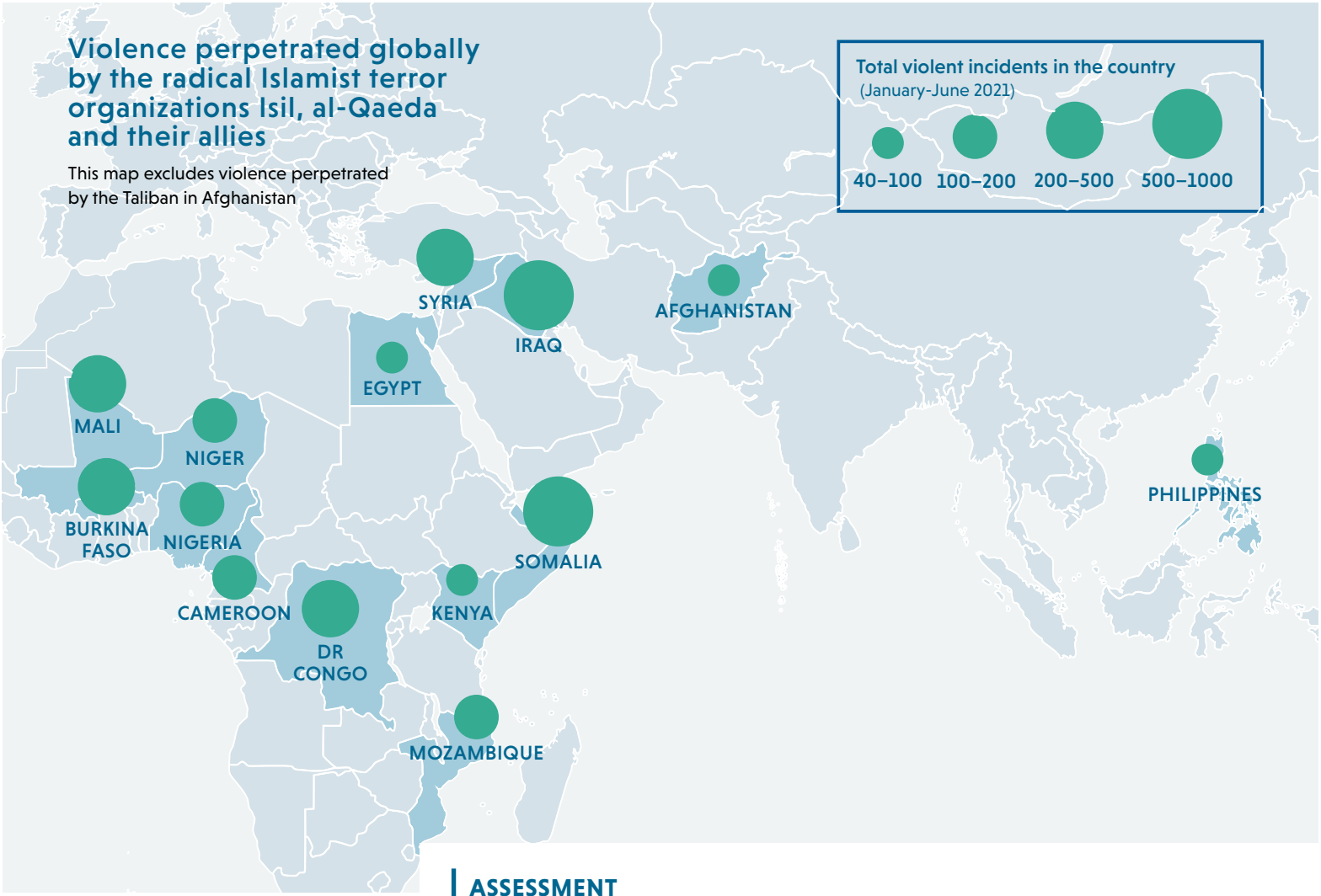
Terrorism

The main threat of terrorism in Finland is posed by individuals and small groups supporting far-right or radical Islamist ideologies. The number of CT targets has remained unchanged at about 390. These CT targets have extensive mutual networks and links to foreign terrorist operators. A significant part of their networking and other activities take place online and using communication applications.

Extreme right-wing terrorism remains a threat in Western countries. The latest serious attack occurred in June, when four people died in an act of violence against Islam in Canada. Some indications have also emerged in Finland concerning the preparation of concrete action since 2019. Far-right terrorist attacks remain possible in the West over the short term, and the likelihood of an attack occurring in Finland cannot be ruled out.

The most significant radical Islamist terrorist organisations globally remain the Islamic State (ISIL) and al-Qaeda. These organisations still pose a global threat, and are also likely to inspire lone operators to mount attacks in Europe. While the central leadership of ISIL is no longer able to direct the global operations of this organisation effectively, its affiliates remain active in conflict zones and fragile states. Al-Qaeda has focused on supporting its regional wings and allies in recent years. The activities of both organisations have increased, particularly in sub-Saharan Africa. Although radical Islamist operators view the re-establishment of a Taliban regime in Afghanistan as a victory, these events are unlikely to have any direct impact on Finland's security situation in the near future.

Although radical Islamist terrorist activities in Finland mainly take the form of supporting operations, such as raising funds and disseminating propaganda and radical ideology, attacks are also possible. The radical Islamist networks of Finland have also previously recruited foreign terrorist fighters for conflict areas, and there are people living in Finland who have participated in and promoted the activities of armed groups.



The threat of far-left terrorism in Finland remains minimal. A few volunteers from Finland have travelled to the Syrian-Iraqi conflict zone to join armed organisations of Kurdish background. The operations of these organisations are mainly directed outside Finland.

ASSESSMENT

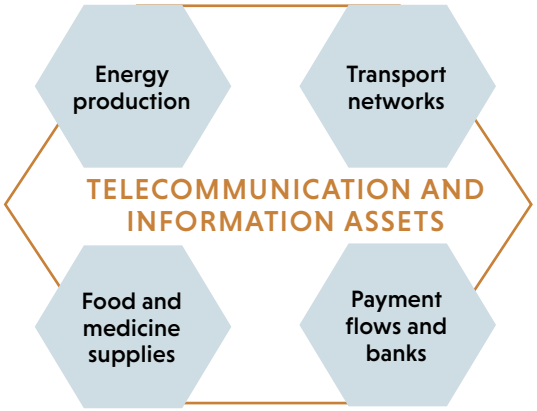
The threat of terrorism is likely to remain at level two (elevated) on the four-level scale in the short term. Individuals or small groups are interested in mounting a terrorist attack in Finland. More people are likely to return to Finland from the Syrian-Iraqi conflict zone, which is very likely to strengthen radical networks in Finland and Europe. Terrorist attacks elsewhere in the West may also affect the terrorism situation in Finland.

Threats to critical infrastructure

Critical infrastructure is a long-term target of foreign intelligence operations in Finland. Authoritarian states can also access Finland's critical infrastructure through legitimate activities, such as business acquisitions and joint ventures.

Operators from authoritarian states have been interested in investing in Finland's fixed infrastructure, but few such investments have been made to date. Besides traditional fixed infrastructure, such as real estate and production facilities, critical infrastructure also includes telecommunications, and the data required for information networks and managing critical infrastructure.

Finnish network infrastructure projects have attracted the interest of operators from China and other countries.



ASSESSMENT

Interest in infrastructure and telecommunication investments will probably continue. The risk to the information infrastructure is particularly high, as this can give authoritarian administrations access not only to the infrastructure itself, but also to Finnish information. Increased monitoring of business acquisitions and investments will probably hamper the ability of authoritarian states to invest in critical functions in Finland.

Dual-use products and weapons of mass destruction

Parties seeking to procure weapons of mass destruction and components of such weaponry have directed efforts through Finland and Finnish operators. They also seek to use Finland as a route for obtaining export-controlled dual-use items and other sensitive technology through individual businesses and procurement networks.

Dual-use items are technologies, services and products that are not only capable of serving civilian uses, but also have military applications. Businesses require a special licence to export controlled dual-use items to destinations outside the European Union. Efforts have been made to exploit business acquisitions, research partnerships and other operations in order to circumvent such export restrictions.

Foreign powers are seeking to boost the technological development of their armed forces through procurement and foreign expertise. Quantum technology and the components required for a quantum computer are one field of technology that is targeted in Western countries, including Finland.

ASSESSMENT

No change to Finland's role in the dual-use item supply chain is likely in the short term. Superpowers actively apply export restrictions as a key component of international policy, with new technologies and organisations likely to be subject to export controls in the short term.

SUPO

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