ULKOPOLIITTINEN INSTITUUTTI
UTRIKESPOLITISKA INSTITUTET
THE FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

November 2013

FIIA COMMENT 15/2013

Mika Aaltola
Programme Director
The Finnish Institute of International Affairs

Finland should aim to be a cyber connector > Finding the right balance between security and privacy calls for careful consideration

Finland forms an integral part of the regional cyber infrastructure. Instead of burying its head in the sand, it should take advantage of its position. Resource allocation, the legal framework, and the oversight of cyber activities all call for a cross-cutting rethink.

The United States is the hub of digital information flows. Cyberspace functions according to the least costly solution, not according to the logic of geographical proximity. American digital companies, such as Amazon, Apple, Microsoft, and Google, have built efficient digital infrastructures, which are so all-embracing that an email sent within Finland is likely to pass through a US-affiliated company. This gives the US a unique advantage regarding its opportunities to conduct cyber surveillance, but other countries are racing to develop their own security, surveillance and espionage capabilities.

Some countries, such as Brazil and Germany, are reacting to this US dominance by looking at how their citizens' online information can be stored on domestic servers. Besides being expensive and technically difficult, these efforts may lead to the "Balkanization" of cyberspace.

Many cyber surveillance activities take place by "tapping" into optical fibre cables and their nodal points, through which the digital information travels. This provides access to all the data passing through the cables.

According to the revelations brought to light by former CIA employee Edward Snowden, the US has managed to place tapping filters in the main physical arteries of the global internet. China, Russia, and other states and transnational actors are also active in this new Great Game.

Finland also occupies a significant position in the cyber connections of the Baltic Sea region, with its geographical location conferring certain advantages that enhance its attractiveness as a location for cyber activities. Finland is free of major tectonic activity and natural catastrophes. Its temperate climate naturally cools down cloud computing farms. It can also offer relatively cheap energy. Google, for example, has invested hundreds of millions of euros in its data centre in Hamina on the south coast of Finland.

The Baltic Sea is a major conductor of data, being criss-crossed by submarine cables that stitch together an important corner of the global cyberspace. For Finland, the most strategically important links are the two BCS North cables that link Russia to Sweden and beyond via Finnish nodal points.

The upshot of this is that a large percentage of Russia's cyber flow with the rest of the world takes place through Finland. Should an outside actor manage to spy on this data traffic, it could lead to mistrust. Russia might then consider counter-reactions or try to bypass Finland in its connections.

Major challenges consequently exist, to which Finland needs to find strategic answers. On the one hand, it should aim to provide a trustworthy and secure haven for cyber-related investments. On the other hand, it needs to safeguard its own cyber security. To some extent, these goals may even be contradictory.

First, Finland needs to diversify its access. The planned direct cable to Germany should be a priority. Similarly, a cable connection across the Arctic to Asia would support Finnish digital resilience.

There are also factors favouring increased cooperation with Sweden or adapting its 'active' practice and the legal framework on cyber surveillance. According to media reports, Sweden has been instrumental in alerting Finland to the recent major cyber-espionage case where the Finnish foreign ministry was infiltrated. However, Swedish and Finnish interests do not always converge. One should keep in mind that the Swedish authorities are able to access most of the digital data sent by Finns.

In addition to Sweden, Finland needs to cooperate in surveillance activities with the United States and its allies. The realities of cyber-

geopolitics and the chronic lack of resources create pressures for smaller states such as Finland to collaborate with the so-called five eyes – the US, the UK, Canada, New Zealand and Australia.

At the same time, very tight integration with these states might lead to growing suspicions by other actors, attempts to bypass Finland as a cyber connector, and to more direct and offensive cyber-related counter-measures. Business investments from the non-Western world could also suffer. Finland should therefore exercise prudence when it comes to pinpointing where its own interests and those of its close collaborators converge, and where they do not.

Another crucial issue is the parliamentary oversight of cyber surveillance efforts. Here, legislation is needed that allows cyber-related governmental actors to fulfil and coordinate their tasks effectively. In all of these vital aspects Finland lags behind comparable states like Sweden. In the age of global terrorism and crime, international cooperation between intelligence agencies is active. Sometimes under-the-radar collaborations are also needed, some of which might incur serious political risks and liabilities.

Finland has to be both vigilant and poised to deter potential harmful actions. At the same time, it has to be mindful of maintaining its trustworthy reputation and safeguarding privacy issues. Individual internet users and their perceptions can lead to consumer reactions or cyber protests against countries that are seen to be violating the rights of their netizens.

Securely managed Finnish connectivity requires a resilient, well-functioning, and rule-abiding society with well-maintained international interoperability based on international best practices and the highest standards.

Finnish Institute of
International Affairs
Kruunuvuorenkatu 4
PL 400
00161 Helsinki

Telephone
+358 (0)9 432 7000

Fax
+358 (0)9 432 7799

www.fiia.fi