Krzysztof Kaczmarek[*]

Finland in the light of cyber threats in the context of Russia's aggression against Ukraine

Abstract

Russia's attack on Ukraine on 24 February 2022 caused Finland to put an end to its long-standing policy of finlandization and to make a decision to join the North Atlantic Treaty Organisation. Intensified Russian-inspired cyber-attacks against Finland were expected. However, over the first three quarters of 2022, no major cyber incidents occurred. In this article, the Author will undertake an attempt to answer the question as to how Finland and Finnish society defend themselves against cyber threats and whether the lack of any recorded attacks from Russia is the result of Finland's level of cyber security or the Kremlin's lack of interest in such activities.

Key words: Finland, Russia, Ukraine, NATO, security policy, cyber attack

[*] Krzysztof Kaczmarek, PhD, Faculty of Humanities, Koszalin University of Technology, e-mail: puola@tlen.pl, ORCID: 0000-0001-8519-1667.

Introduction

Finland's application for membership in the North Atlantic Treaty Organisation (NATO) has increased the level of a threat of cyber attacks from Russia. As early as at the beginning of March 2022, Finnish services reported possible attempts by the Kremlin to interfere with Finnish public opinion. The warnings included the possibility to use both traditional and new methods, such as deep fake video[1].

In Finland, approximately 1.5 million firearms are legally in private hands. The vast majority of these include hunting weapons, but their widespread possession is also seen as a factor that increases the country's defence capability[2].

The decision to join NATO explicitly demonstrated that there was an end to many decades of the finlandization policy. After Russia's attack on Ukraine, Finland's geopolitical position changed, and an all-encompassing security strategy, based on a highly digitalised society, revealed its weaknesses. Since so many Finns possess weapons, and the country is highly digitalised, there is unfortunately a fairly high risk that Russia may already have a list of Finns with gun permits or hunting licences[3].

According to Supo (the Finnish police service responsible for the state's internal security), the worst threats to Finland's national security at the moment include Russia's extensive influence and an illegal accumulation of intelligence data. Cyber threats hit the headlines with the Russian war of aggression in Ukraine, and public interest in cyber security increased even more after Finland decided to apply for NATO membership[4].

At the same time, Finland has been preparing for cyber threats for many years by running regular drills involving both public and private entities. Their purpose is to strengthen liaison between companies and authorities in the

[1] D. Mac Dougall, *Deep fakes and blackmail: Finland warns Russia could meddle in NATO membership debate*, https://www.euronews.com/2022/03/30/deep-fakes-and-blackmail-finland-concerned-about-russian-interference-in-nato-debate [access: 18.09.2022].

[2] *Aseiden määrä Suomessa vähenee – katso, missä ovat maan 1,5 miljoonaa asetta*, https://yle.fi/uutiset/3-8588611 [access: 20.09.2022].

[3] S. Czubowska, *Finlandia preppersem Europy. W cyberprzestrzeni zbroi się przed Rosją*, https://spidersweb.pl/plus/2022/06/finlandia-rosja-nato [access: 18.09.2022].

[4] S. Hotakaisen, *Älä mene verkossa lankaan – todennäköisesti suuri perintö on huijaus*, https://www.keskipohjanmaa.fi/uutinen/640404 [access: 20.09.2022].

event of large-scale cyber incidents[5]. It would therefore appear that Finland, in terms of cyber threats, is a country of preppers. It is therefore worth examining some elements of the country's preparedness for digital threats.

Global trends in the use of digital tools against states

Harmful activities in cyberspace may take place in three ways: 1) intelligence (espionage); 2) attacks; 3) data manipulation (processing)[6]. Cyber espionage is similar to traditional intelligence and espionage activities, which aim to collect information. Data stolen and collected through cyber-intelligence may be kept secret or made public to influence public opinion and governments in a hybrid impact[7].

Two well-known hacker groups (APT 28/Fancy Bear and APT 29/Cozy Bear) linked to Russian intelligence services are known to have carried out espionage operations on computer networks against other countries. In 2015, APT 29 infiltrated the US White House information network and, in addition, the networks of several organisations in Western Europe, Central and East Asia as well as Central and South America. APT 28 was also found to have hacked into the networks of military and defence companies in the Americas, Europe and Asia. It was also behind hacks into the networks of the German Reichstag and France's TV5 Monde in 2015. Covert data collection is nothing new, but the cyber dimension brings new tools and lower costs. Cyber operations are inexpensive, the risks are low and they may produce good results. This makes cyber tools attractive for poorer countries, as well. A cyber-attack is a continuum of cyber-intelligence and it refers to an attack that targets the cyber infrastructure of the electricity, communications, water, financial and critical systems of society. To date, there have been relatively few such attacks, but this activity has increased significantly in recent years[8].

[5] *Suomessa alkaa jättimäinen viranomaisten kybersotapeli, jonka käsikirjoituksesta ei hiiskuta julkisuuteen – Mukana 120 organisaatiota*, https://yle.fi/uutiset/3-12629560 [access: 20.09.2022].

[6] J. Kurek, *Challenges for State Security in the Context of Big Data Analysis* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022, p. 62.

[7] *Kyberuhat ja Tietoverkkovaikuttaminen*, https://turpopankki.fi/uusia-turvallisuushaasteita/hybridi-ja-kybervaikuttaminen/kyberuhat-ja-tietoverkkovaikuttaminen/#toggle-id-2 [access: 18.09.2022].

[8] Ibidem.

The discovery of the Stuxnet virus in 2010 on Iranian computer systems marked the realisation of a new kind of a cyber warfare method. This „world's first digital weapon" differed from previous spyware in that, in addition to stealing data, it destroyed physical devices controlled by computers. There were two different versions of the attack: the first one damaged the centrifuges of Iran's uranium enrichment facilities and the second one manipulated the companies' computer systems. The companies in question supplied industrial control and processing systems for Iran's nuclear programme[9].

One of the most worrying attacks included a successful attack on the computer network of Telvent (a Canadian company) by the 61398 Unit (APT 1/Comment Crew/Comment Panda). The company designs remote access software for valves, switches and security systems for oil and gas companies and power grid operators. Telvent maintains detailed plans for more than a half of all oil and gas pipelines in North and South America and it has access to their systems. Cyber attacks on critical infrastructure, especially energy grids, have occurred in the context of almost all of the recent political and military crises, among others. In 2007 in Estonia, in 2008 in the Balkans and in Georgia, in Ukraine since 2014, in Syria and elsewhere in the Middle East[10].

In cyber manipulation, groups of hackers may manipulate or alter data stored on a computer network once it has entered the system. Manipulation could be a major challenge in the future. To date, most intrusions into computer networks include data theft. The threat is that an intruder will begin to manipulate and alter data so that the network owner may no longer believe and trust their own system. James Clapper, the former US Director of National Intelligence (DNI), expressed his concern by saying, „I believe we will see more cyber operations that alter or manipulate electronic information to compromise its integrity". One of the most serious incidents of electronic manipulation occurred in 2013, when Syrian hackers accessed the Twitter account of the Associated Press news agency and tweeted fake news about an explosion at the White House. This also had a direct impact on interest rates on the US stock market. One of the first attempts to manipulate data to achieve political ends occurred during the 2016 US presidential election. Russian hackers who gained access to the Illinois voter database attempted to alter the electoral roll data, yet without any success[11].

[9] Ibidem.
[10] Ibidem.
[11] Ibidem,

In 2017, there occurred a lot of ransomware (ransomware; WannaCry, NotPetya and BadRabbit) in an almost epidemic fashion. In 2018, it was revealed how inadequate the capabilities are to face cyber threats related to side-channel attacks and vulnerabilities in microprocessors as well as in various components and devices (infringed components). In the year 2019, covert military operations related to interstate conflicts started to take place in cyberspace. For this reason, cyber threat researchers around the world have begun to shift their focus from financially motivated cyber criminals to state-sponsored cyber operations. In the recent years, the Internet of Things has introduced a new dimension to the cyber world that can be used in cyber operations. Due to the low level of security of devices, it is possible to access computer networks and spread malware through these[12].

Governments' activities in cyberspace

The cyber activities on the part of governments and the groups they support are primarily focused on intelligence. There are more than a hundred active groups worldwide, which have been linked to organisations in almost 20 countries. These organisations include South Korea, India, Iran, Israel, Lebanon, Nigeria, Pakistan, Palestine, North Korea, Syria, Russia, Vietnam, Turkey, the United Arab Emirates and the United States, among others. Several Western countries, such as the UK, France, Germany and the United States, operate in cyberspace with actors involved in intelligence and defence organisations[13].

Cyber operations, in combination with other means of hybrid influence, have created opportunities for governments to act in ways that can be carried out, at least to some extent, in secret and in such a way that states' involvement in matters that come to light can be denied. Offensive cyber operations were used in particular in the context of the crisis in Ukraine and the occupation of Crimea, as well as in the Middle East in the context of the Syrian civil war and the situation in Iran[14].

From among government-sponsored cyber operators, Russian actors are the most active ones and have caused the worst damage. Since 2014, their main

[12] Ibidem.
[13] Ibidem.
[14] Ibidem.

target has been the Ukrainian government and its law enforcement and armed forces. Since 2017, Russian actions have also targeted critical infrastructure and the energy sector in Europe and the United States, such as nuclear power plants. At least seven Russian groups, operating under different names, have been identified[15].

Chinese groups have been observed to be oriented towards the requirements set out in the government's Made in China 2025 plan for the technology, energy and healthcare sectors. There has been an increase in the activities of the Chinese groups in recent years, which is at least partly related to the deterioration of the US-China relations[16].

In recent years, Iranian groups have intensified their operations owing to new tactics, techniques and procedures. These include, for example, strategic hacking campaigns and mobile malware. These have been used against regional rivals to constrain the opposition's activities at home, as well as to support their own „soft war" campaigns. North Korean groups have also increased their activity recently. Their areas of interest include mainly the financial sector and intelligence targeting South Korea[17].

Expert recommendations to Finnish society in the event of a large-scale cyber incident

Cyber threats are not bound by place, time or national borders, and improper conduct or damage does not always meet the criteria of a crime under existing national laws. This is particularly true for disinformation activities. Since the Russian invasion of Ukraine, the European Union has imposed a series of harsh sanctions on Russia, and some Kremlin-controlled news services have lost their ability to broadcast in the territory of the Community. However, Russian-language search results on Apple and Google still mainly include news sources spreading Kremlin propaganda[18].

[15] Ibidem.

[16] Ibidem.

[17] Ibidem.

[18] J. Kullas, *Noudattavatko teknologiajätit Venäjä-pakotteita? Applen Siri mainostaa Kremlin propagandaa*, https://www.mikrobitti.fi/uutiset/noudattavatko-teknologiajatit-venaja-pakotteita-applen-siri-mainostaa-kremlin-propagandaa/5c661f7c-2863-4863-aea5-12261a2707eb [access: 18.09.2022].

Based on historical experience, Finnish society has long been preparing for crisis situations. At the same time, procedures for dealing with emergency situations are being developed on an ongoing basis. Following Russia's attack on Ukraine and Finland's declaration to join NATO, Finnish-Russian relations have cooled considerably.

According to Finland's Traficom National Cyber Security Centre, the number of cyber threats to Finland will increase as the country joins the North Atlantic Treaty Organisation[19].

One of the signals of an incipient Russian cyber-attack on Finland is likely to be a disinformation campaign referring to history and portraying past events in a light intended to cause social division and to discredit Western countries in the eyes of Finnish society. Similar incidents took place in Estonia in 2007. There was civil unrest at the time and the country was subjected to numerous cyber attacks. At the same time, immediately prior to the military attack, Russia inspired a number of cyber attacks on Ukraine[20].

The Finnish authorities are preparing the public for cyber attacks on the assumption that the most effective disruption to the normal functioning of the state may be caused by the technically simplest „denial of service" attacks, which cause online services to fail. Immediately prior to the attack, Russia had attacked Ukraine's financial, telecommunications, software, energy and healthcare sectors in this way. In addition, water supply, trade and distribution sectors were attacked, including the media sector[21].

Regardless of the global geopolitical situation, an increase in the number of attempted cyber attacks on Finland has been observed since the beginning of 2019, but these have not been successful. In spring 2022, however, there were a few rare „denial of service" attacks on government websites in Finland. A „denial of service" attack puts so much strain on a company or organisation's public website that its network crashes. In addition, GPS signal jamming was observed in Finland during that same period[22].

It seems that most of Finnish society are prepared to reduce the impact of cyber attacks by following several basic principles. Finnish experts indicate that society will be prepared for cyber attacks provided that every citizen is

[19] *Näin sinä voit varautua mahdollisen Nato-jäsenyyden aiheuttamiin kyberuhkiin – listaamme kuusi tapaa*, https://yle.fi/uutiset/3-12440524 [access: 21.09.2022].

[20] Ibidem.

[21] Ibidem.

[22] Ibidem.

prepared. To this end, they recommend first and foremost that every household should have enough provisions to function for at least a few days without any additional supplies[23].

They also point out that any type of an attack on the banking sector may result in an inability to use services that require bank identification to log in, such as the police or health care system. The impact of such attacks can be reduced by using the services of two different banks. One should also perform activities that require bank identification well in advance of the deadline. Mobile verification can also be used, but again, it is safer to have two SIM cards from different operators[24].

In the majority of cases, Finns follow the recommendations on what steps to take when electronic payment systems (including cards) are not working by possessing enough cash for expenses necessary for a period of a few days. However, the recommendations are to have both payment cards from two different banks and cash[25].

According to experts, considering the level of preparedness on the part of energy companies, a denial-of-service attack is unlikely to cause power outages in Finland. However, even this is not completely out of question. Therefore, they recommend having an emergency power source, e.g. a power bank. It is also recommended to have a battery-powered radio, as it may be the only source of information in the event of a crisis. In addition to technical aspects, it is also disinformation campaigns that may have serious consequences. Finns are alert to this possibility especially in the context of Russia's aggressive policy. The Finnish authorities are sensitising Finnish society particularly to information related to refugees[26].

Countering cyber attacks and their impact in Finland

The most common cyber threats in Finland include ransomware, denial of service attacks and data leaks. Attacks on IT service providers have also become more common. More lasting damage is caused by the destruction of IT systems and data repositories, which also aims to increase uncertainty

[23] Ibidem.
[24] Ibidem.
[25] Ibidem.
[26] Ibidem.

in conflict situations. In order to be prepared for cyber threats, institutions must be able to identify the targets to be protected and determine which of these are the most important ones. What does an organisation need to do to guarantee basic security? Who ultimately has access to strategic data and has the security of the cloud services used by the organisation been thought through to the end? Ensuring cyber security requires answers to these questions. Remote working brings with it new risks associated with a transition from a company-controlled network to unattended networks. In addition, the use of employees' own devices exposes them to security risks[27].

Technical protection provides a solid foundation for cyber security. Criminals often look for easy targets with vulnerabilities. A good firewall is the minimum level at which an institution demonstrates that it is prepared for cyber threats[28]. Good technical security is created by automatic software updates, identified users as well as strong and different passwords for different services. In an increasingly mobile world, it is worth remembering that mobile tools are also vulnerable to security incidents.

Security of administrative information also constitutes one element of being prepared for cyber threats. Good governance and risk management enable smooth operations and minimise potential threats. Research confirms that in Finland, institutions are well prepared for cyber threats, with trainings focused on the knowledge of procedures and their actual implementation in the case of threats.

Conclusions

Russia's attack on Ukraine on 24 Feb. 2022 changed the geopolitical shape of the world. The balance of security also changed. Finland's position on the international stage also changed. Situated on the geographical periphery of Europe, the country has always sought to balance relations between the blocs formed by the superpowers. However, in terms of preventing cyber threats, Finland's line of conduct has not changed. The country's authorities and its

[27] M. Långström, *Mitä organisaatiot voivat tehdä varautuakseen kyberuhkiin?*, https://www.rakli.fi/rakli-tiedottaa/mita-organisaatiot-voivat-tehda-varautuakseen-kyberuhkiin/ [access: 21.09.2022].

[28] W. Pizło, *Management in Cyberspace: From Firewall to Zero Trust* [in:] *The Public Dimension...*, p. 141.

society seem to be prepared for most attacks taking place in cyberspace. This is most certainly due to the historical experience of Finland, which has been exposed to threats from its eastern neighbour for centuries and, in particular, in the 20th century. Both Finland's domestic, foreign and security policies are multifaceted and are constantly evolving, and in the era of cyber society, cyber security has become an integral part of national security[29]. Apart from some spectacular attacks, such as the suspension of the Parliament's website, there is no widely known information concerning serious cyber-attacks on Finland. There seem to be three possible explanations for this: 1) Finland is perfectly prepared and repels all attacks; 2) successful attacks are concealed; 3) the possibilities of Russia's hostile cyber activities are overestimated.

Obviously enough, Russia should not be underestimated, yet being aware of threats makes it possible to counter them and minimise any potential losses in the event of a successful cyber attack. Therefore, Finland appears to be a country that is well prepared for cyber threats.

Bibliography

Aseiden määrä Suomessa vähenee – katso, missä ovat maan 1,5 miljoonaa asetta, https://yle.fi/uutiset/3-8588611 [access: 20.09.2022].

Czubowska S., *Finlandia preppersem Europy. W cyberprzestrzeni zbroi się przed Rosją*, https://spidersweb.pl/plus/2022/06/finlandia-rosja-nato [access: 18.09.2022].

Hotakaisen S., *Älä mene verkossa lankaan – todennäköisesti suuri perintö on huijaus*, https://www.keskipohjanmaa.fi/uutinen/640404 [access: 20.09.2022].

Kullas J., *Noudattavatko teknologiajätit Venäjä-pakotteita? Applen Siri mainostaa Kremlin propagandaa*, https://www.mikrobitti.fi/uutiset/noudattavatko-teknologiajatit-venaja-pakotteita-applen-siri-mainostaa-kremlin-propagandaa/5c661f7c-2863-4863-aea5-12261a2707eb [access: 18.09.2022].

Kurek J., *Challenges for State Security in the Context of Big Data Analysis* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

Långström M., *Mitä organisaatiot voivat tehdä varautuakseen kyberuhkiin?*, https://www.rakli.fi/rakli-tiedottaa/mita-organisaatiot-voivat-tehda-varautuakseen-kyberuhkiin/ [access: 21.09.2022].

Mac Dougall D., *Deep fakes and blackmail: Finland warns Russia could meddle in NATO membership debate*, https://www.euronews.com/2022/03/30/deep-fakes-and-blackmail-finland-concerned-about-russian-interference-in-nato-debate [access: 18.09.2022].

Näin sinä voit varautua mahdollisen Nato-jäsenyyden aiheuttamiin kyberuhkiin – listaamme kuusi tapaa, https://yle.fi/uutiset/3-12440524 [access: 21.09.2022].

Pizło W., *Management in Cyberspace: From Firewall to Zero Trust* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

[29] D. Tyrawa, *The Axiological and Legal Aspects of the Multi-faceted Nature of Cybersecurity* [in:] *The Public Dimension...*, p. 23.

Suomessa alkaa jättimäinen viranomaisten kybersotapeli, jonka käsikirjoituksesta ei hiiskuta julkisuuteen – Mukana 120 organisaatiota, https://yle.fi/uutiset/3-12629560 [access: 20.09.2022].

Tyrawa D., *The Axiological and Legal Aspects of the Multi-faceted Nature of Cybersecurity* [in:] *The Public Dimension of Cybersecurity*, eds. M. Karpiuk, J. Kostrubiec, Maribor 2022.

Finlandia wobec cyberzagrożeń w kontekście agresji Rosji na Ukrainę

Streszczenie

Atak Rosji na Ukrainę 24 lutego 2022 roku spowodował, że Finlandia skończyła z długoletnią polityką finlandyzacji i zdecydowała się na przystąpienie do Paktu Północnoatlantyckiego. Spodziewano się skierowanych przeciwko niej zintensyfikowanych ataków cybernetycznych inspirowanych z Rosji. Jednakże przez pierwsze trzy kwartały 2022 roku nie doszło do żadnych poważnych incydentów cybernetycznych. W artykule autor podjął próbę odpowiedzi na pytania: w jaki sposób Finlandia i społeczeństwo tego państwa bronią się przed cyberzagrożeniami oraz czy brak odnotowanych ataków ze strony Rosji jest skutkiem poziomu cyberbezpieczeństwa Finlandii czy też braku zainteresowania Kremla takimi działaniami.

Słowa kluczowe: Finlandia, Rosja, Ukraina, NATO, polityka bezpieczeństwa, cyberatak