Krzysztof Kaczmarek*

Nordic Countries in the Face of Digital Threats

Abstract

Technological advances and the digital revolution have caused much of social activity to move online. The Internet has become a tool without which it is difficult to imagine the functioning of modern states. However, it is also some of conflicts between states that have moved online, and states with the highest degree of digitization, which include the Nordic states, have become a target of attacks by other states or organizations.

In this article, the Author will attempt to answer the question of how the Nordic states and their societies defend themselves against cyber threats. The characteristics of the attacks carried out against them and the levels of digitization of the societies will also be compared.

Key words: Nordic cooperation, cyber threats, digital skills, DDoS (Distributed Denial of Service)

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

Introduction

Addressing information security and cyber security issues requires close and multi-faceted cooperation between units, institutions and states, as no single entity is able to counter threats alone. This cooperation is most frequently based on the common interests of various entities, such as groups of states. One such group is the Nordic states, whose cooperation in many areas has taken various forms over the past centuries. The origins of formal agreements and accords date back as far as the 14th century. However, it was not until after World War II that Nordic cooperation took an institutionalized form of cooperation that was organized and based on an exchange of mutual benefits. In order to strengthen regional ties, the countries of northern Europe entered into institutionalized cooperation in 1952 within the framework of the Nordic Council[1].

There is a consensus in the literature that the Nordic countries' cooperation is based on shared values, ties and history[2]. The members of the Nordic Council, which is a body of inter-parliamentary cooperation between the Nordic states, include representatives of the Parliaments of Sweden, Denmark, Norway, Finland, Iceland and dependent territories, i.e. the Åland Islands, the Faroe Islands and Greenland[3].

All of the Nordic states are highly digitized and, as a result, one of their obligations is to maintain the cyber resilience of societies (understood here as an ability of critical societal functions to withstand and overcome the negative effects of unexpected events originating in cyberspace). Since governments' direct control over society is limited in democratic states, they carry out this task in private-public cooperation using the principle of sectoral responsibility. The experience of all the Nordic states indicates that effective implementation of the sectoral responsibility principle in the cyber area is a major challenge, and that these states need a more explicit division of tasks and responsibilities to strengthen their resilience to digital threats[4].

1 M. Gębski, *Rada Nordycka – regionalna „Unia" na Północy*, 2021, https://www.forum-ekonomiczne.pl/publication/rada-nordycka/ [accesse: 10.09.2023].

2 M. Tomala, *Współpraca międzyparlamentarna Rady Nordyckiej z perspektywy konstruktywizmu*, „Przegląd Sejmowy" 2019, no. 5, p. 85.

3 Ibidem, p. 86.

4 M.S. Jensen, *Cyberresiliens, sektorprincip og ansvarsplacering – nordiske erfaringer*, „Internasjonal Politikk" 2019, vol. 77, no. 3.

Nordic cooperation in the area of cyber security has taken on new importance in the context of Russia's attack on Ukraine and Finland's accession to the North Atlantic Treaty Organization (NATO). This is especially so since Russia, as part of its neo-imperialist policy, considers Finland to be its sphere of influence. Sweden, on the other hand, is still (as of Sept. 10, 2023) waiting for its accession to NATO to be accepted by all the members of the alliance. However, due to their traditions of cooperation, joint countering of cyber threats in the Nordic countries is not always formal and it often takes place at different levels.

The purpose of the article is an attempt to analyse the ways in which the Nordic states protect themselves against digital attacks that, for largely digitized societies, may have effects comparable to the use of conventional weapons on their territories.

Nordic Defence Cooperation

The origins of Nordic defence cooperation date back to the 1960s. Initially, it involved an exchange of information and joint peacekeeping activities, and duties were distributed between the peacekeeping training centres: Denmark was responsible for military police courses, Finland trained military observers, Norway was responsible for logistics specialists and Sweden for staff officers. As part of this cooperation, three separate structures were established in the late 20th and early 21st centuries: the Nordic Armaments Cooperation (NORDAC) in 1994, the Nordic Coordinated Arrangement for Military Peace Support (NORDCAPS) in 1997 and the Nordic Supportive Defence Structures (NORDSUP) in 2008. These structures were merged into one in 2009: the Nordic Defence Cooperation (NORDEFCO)[5].

According to the Finnish Foreign Ministry, Nordic security policy cooperation includes activities related to modern technologies, among other

5 *The Nordic Defence Cooperation (NORDEFECO)*, https://www.defmin.fi/en/areas_of_expertise/international_defence_cooperation/nordic_defence_cooperation#b67ddad9 [access: 8.09.2023].

things[6]. At the same time, cooperation on cyber security within NORDEFCO takes place in close cooperation with the United States[7].

The military level of NORDEFCO is divided into five Cooperation Areas: capabilities, armaments, human resources and education, training and exercises as well as operations. Cyber defence is included in capabilities[8]. In a longer term, the cooperation is expected to involve, among other things, increased intelligence sharing among members, which is expected to improve their ability to defend against threats, including those from cyberspace[9]. In all of the Nordic countries, digital security relies heavily on cooperation between public and private sectors. However, it should be noted that, despite close cooperation and some commonalities, the Nordic countries are not unanimous concerning cyber security. This applies both to national and individual level activities.

Cyber threats in the Nordic countries

In order to analyse ways to increase the level of cyber security in the Nordic countries, it is necessary to compare what types of cyber-attacks are carried out against them. It may also be helpful to compare the levels of digital competence in the societies and the degree of digitization of social services.

Finland: According to information provided by Finnish experts, cyber-attacks in Finland most often target institutions and organizations rather than individuals (who may, however, be affected by such an attack). The most common cases include phishing and distributed denial of service attacks (DDoS). At the same time, 2022 saw increased attacks on critical infrastructure. Public institutions refrain from explicitly indicating Russia's involvement. However, for example, in interviews, those in executive positions in these institutions

6 *Pohjoismainen ulko- ja turvallisuuspoliittinen yhteistyö*, https://um.fi/pohjoismainen-ulko-ja-turvallisuuspoliittinen-yhteistyo [access: 8.09.2023].

7 *Press release of the U.S.-Nordic Leaders' Summit in Helsinki on 13 July 2023*, https://www.presidentti.fi/en/press-release/press-release-of-the-u-s-nordic-leaders-summit-in-helsinki-on-13-july-2023/ [access: 8.09.2023].

8 *The Cooperation Areas*, https://www.nordefco.org/The-Cooperation-Areas [access: 8.09.2023].

9 *Wojna dała impuls. Państwa nordyckie rozwijają cyberobronę*, https://cyberdefence24.pl/polityka-i-prawo/wojna-dala-impuls-panstwa-nordyckie-rozwijaja-cyberobrone [access: 8.09.2023].

point to Finland's eastern neighbour while not ruling out an involvement of China or international criminal groups[10].

As much as 40% of the adult population in EU countries is at risk of digital exclusion. Those aged 25–64 rate their digital skills as poor; they rarely or not at all use the Internet. This is according to the report known as Adult Education and Training in Europe, published by the European Commission's Eurydice network in early autumn 2021, which compares adult education and its structures in Eurydice network member states.

In Finland, the situation is clearly better than the European average. The percentage of adults with low or no digital skills is the third lowest among the countries compared. Ca. 15% of Finland's adult population rated their digital skills as poor. Only 2% of Finnish adults had not used the Internet in the last three months before the survey, while in Bulgaria, for example, the percentage was as high as 25%[11].

Denmark. According to the Centre for Cybersikkerhed, Denmark's national cybersecurity body, the most serious threats to Denmark in the digital area include cyber espionage (especially from Russia and China) and DDoS attacks. Financially motivated attacks on companies and individuals are also common, and the criminals carrying them out are opportunistic and not affiliated with any country[12]. There is also the threat of attacks on critical infrastructure, especially in the context of Denmark's membership in NATO and the EU, and the country's active participation in a broad support offered to Ukraine in its war with Russia. Especially since during significant crises, operations in the information technology sector can serve as an additional means of influence, supporting conventional armed forces[13].

According to the European Commission's 2021 report, Denmark is the most digitized country in Europe, followed by Finland and Sweden[14]. Denmark ranks fourth among EU countries in terms of its overall digital competency

10 J. Vildhjärta, *Pestel-analyysityökalun luominen organisaation kyberturvallisuuden tueksi*, Tornio–Rovaniemi 2023, p. 21.

11 *Eurydice-raportti: Suomalaisten aikuisten digiosaaminen on Euroopan kärkipäätä*, https://www.oph.fi/fi/uutiset/2022/eurydice-raportti-suomalaisten-aikuisten-digiosaaminen-euroopan-karkipaata [access: 8.09.2023].

12 *Cybertruslen mod Danmark 2023*, København 2023, p. 4–7.

13 M. Karpiuk, W. Pizło, K. Kaczmarek, *Cybersecurity Management – Current State and Directions of Change*, „International Journal of Legal Studies" 2023, no. 2, p. 647.

14 *Redegørelse om Danmarks digitale vækst 2022*, København 2022, p. 9.

index. The same is true for the core index of advanced digital skills, with IT professionals making up more than 5% of the Danish workforce[15].

Sweden. The most common types of cyber-attacks encountered in Swedish institutions are DDoS attacks. At the same time, phishing for private information is popular among criminals. Frequently, these are attempts to extort data allowing access to financial resources. However, there are also cases with no financial motivation: theft of private information and its subsequent publication[16]. The most common cases include data and information on the sphere of sexuality.

According to experts, the most serious problem concerning cyber security in the broadest sense is security gaps in critical infrastructure. The country's authorities are working to improve this situation but, understandably, information on this is not disclosed[17].

In terms of digital competences, 66,5% of Sweden's adult population have at least basic digital skills, which is comparable to the average of 53,9% in the European Union[18]. At the same time, according to Swedish experts, the competences of the country's population present a „double picture", i.e. Sweden is at the forefront internationally, while at the same time a large part of the population lacks basic digital skills[19].

Norway. Norway has been experiencing targeted attacks on critical infrastructure, according to experts, and cyberattacks are one of the most serious threats to the country's security. These attacks are most often invisible and difficult to detect, and are aimed at gaining control of systems. This may make acts of sabotage or terrorism easier to carry out[20]. This, in

15 Ibidem, p. 45–46.

16 *Cyber mot Sverige*, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwjF_rTewqCBAxX5GBAIHYcDBvsQFnoECB0QAQ&url=https%3A%2F%2Fwww.ri.se%2Fsites%2Fdefault%2Ffiles%2F2022-09%2FRapport%2520Cybers%25C3%25A4kerhet.pdf&usg=AOvVaw3jdk2yrwZDtkMWSQejPSFx&opi=89978449 [access: 10.09.2023].

17 M. Alpman, *Sverige under cyberattack*, https://fof.se/artikel/2018/4/under-attack/ [access: 11.09.2023].

18 D. Bogerius, *Digital kompetens en förutsättning*, 2023, https://www.techsverige.se/2023/03/digital-kompetens-en-forutsattning/ [access: 8.09.2023].

19 L. Jönsson, *DIGG-rapporten: en lägesrapport om svensk digitalisering*, 2023, https://digiteket.se/inspirationsartikel/digg-rapporten-en-lagesrapport-om-svensk-digitalisering/ [access: 8.09.2023].

20 *Dataangrep er blant de største truslene mot Norge. Derfor er kraftsektoren et ettertraktet mål*, https://www.tekna.no/kurs/innhold/dataangrep-er-blant-de-storste-truslene-mot-norge.-derfor-er-kraftsektoren-et-ettertraktet-mal/ [access: 11.09.2023].

turn, may lead to attempts to achieve political goals[21]. State institutions and NATO infrastructure located in Norway have also been targets of cyber-attacks. On July 12, 2023, it was revealed that hackers, taking advantage of software vulnerabilities, broke into a computer system used by 12 Norwegian ministries and had access to it for at least two and a half months. The software was used by numerous government and private organizations both in Norway and internationally, including NATO, the Norwegian Coastal Administration and the Royal Palace. However, what is most disturbing is that despite the fact that thousands of companies around the world use the software, it was only Norwegian ministries that confirmed that they experienced computer attacks[22]. Like all highly digitized countries, Norway is a target of DDoS attacks.

Regarding the digitization of Norwegian society, the figures are as follows: 94% use the Internet daily or almost daily, 93% of Norwegians use the Internet several times a day, 1% use the Internet less than once a week. At the same time, 3% of the population are non-users, i.e. they do not use any digital tools or the Internet. Concerning skills, 11% of Norwegians have poor competences. This means that they have little or no experience in solving digital tasks. Digital skills in the population decline with age. It is mainly among those over 60 that we find non-users of online services and those with the lowest levels of digital skills[23].

Iceland. The most common type of cyber-attacks in Iceland is DDoS. Actions aimed at phishing credentials for various services (e.g. banking) are also encountered. However, these actions tend to be global in nature, rather than targeting residents of a specific country.

As regards the digitization of Icelandic society, studies show that almost all households in Iceland now have access to the Internet (96,1%). One of the main challenges in this country is the lack of infrastructure in the majority of rural areas. Despite the increasing availability of broadband services, many rural areas still have difficulty accessing reliable Internet. This is due to insufficient investment in infrastructure in these areas. It also means that residents in

21 F. Radoniewicz, *Zwalczanie cyberterroryzmu w ramach UE – wybrane aspekty karnomaterialne*, „Cybersecurity and Law" 2019, no. 2, p. 199.

22 *Dataangrep i Norge: Hackerne kunne gått til cyberangrep på Nato, Forsvaret og Slottet. De valgte norske departementer*, „Aftenpoften", https://www.aftenposten.no/norge/i/dwBdWO/dataangrep-i-norge-hackerne-kunne-gaatt-til-cyberangrep-paa-nato-forsvaret-og-slottet-de-valgte-norske-departementer [access: 11.09.2023].

23 *Bruk av digitale verktøy og tjenester*, https://www.digdir.no/rikets-digitale-tilstand/bruk-av-digitale-verktoy-og-tjenester/3571 [access: 11.09.2023].

these areas are missing out on the benefits of the Internet, such as the ability to access online services or participate in the digital economy. Another challenge is the affordability of Internet services. As Internet services are becoming more complex, costs may become prohibitive for some households. There is also a lack of competition in the market, which means prices remain high[24].

Although the majority of Icelandic households have access to the Internet, as many as 18% of them remain without any access. This lack of access is most acute among Iceland's rural population, where 25% of households have no Internet access - more than double the national average. This is partly due to the fact that many neighbourhoods have limited broadband access or no access at all. The digital divide is also evident among the country's younger population. A study by the Icelandic Communications Authority found that Icelandic residents aged between 15 and 24 use Internet services much more rarely than other age groups. In addition, the study demonstrated that those with access to the Internet are more likely to use it for entertainment rather than for educational or professional purposes[25].

Conclusions

All the Nordic countries are among the world's leaders in the use of modern technology in daily activities. This allows them to improve the quality of life of their residents; however, it also carries a number of risks arising from it. In highly digitalized societies, even the smallest failure of ICT systems can cause serious consequences. Research results show that each of the Nordic countries has different characteristics in terms of the use of modern technologies; yet, in all of them, the most popular type of cyberattack carried out against them is DDoS attacks, which may be effective precisely in the case of highly digitized countries. A massive DDoS attack may disrupt entire societies and countries. The 2007 attack on Estonia, may serve as an example here, which shut down the websites of all the ministries, two major banks and several political parties, as well as the parliamentary email server[26]. Since nowadays, in

24 M. Franckiewicz, *Internett på Island*, https://ts2.space/nn/internett-pa-island/ [access: 11.09.2023].
25 Ibidem.
26 K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1, p. 148.

most cases, authentication for access to social services is done through online banking, a disruption of any bank's website could result in the loss of access to other network services such as health care, social security, taxes or contacting any office. At the same time, from the perspective of a country's cyber security, the level of digital competences in its population is also important. Global data shows that in 95% of successful cyber-attacks are caused by humans and not hardware[27]. In terms of digital skills, Nordic countries are among the world leaders.

What seems most significant, however, is that in terms of preventing cyber threats, the Nordic countries' policies are multifaceted. Because of the community, they cooperate with each other but also with other countries. Each of them also has its own internal cyber security policy, which involves both building the necessary infrastructure and improving the digital skills of the population. It is only public awareness of threats that makes it possible to prevent them. However, the government and its executive agencies have a fundamental role in ensuring cyber security[28]. This seems to be the case in the Nordic countries.

Another conclusion from the article is that the risks of cyberattack threats are often not discussed at all in favour of, arguably, economic benefits. This is evidenced by the case disclosed by Norwegian authorities of the surveillance of 12 of the country's ministries as a result of security vulnerabilities in software still used by public institutions in other countries, including those responsible for security.

Bibliography

Alpman M., *Sverige under cyberattack*, https://fof.se/artikel/2018/4/under-attack/ [access: 11.09.2023].

Bogerius D., *Digital kompetens en förutsättning*, 2023, https://www.techsverige.se/2023/03/digital-kompetens-en-forutsattning/ [access: 8.09.2023].

Bruk av digitale verktøy og tjenester, https://www.digdir.no/rikets-digitale-tilstand/bruk-av-digitale-verktoy-og-tjenester/3571 [access: 11.09.2023].

Cyber mot Sverige, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwj\F_rTewqCBAxX5GBAIHYcDBvsQFnoECB0QAQ&url=https%3A%2F%2Fwww.ri.se%2Fsites%2Fdefault%2Ffiles%2F2022-09%2FRapport%2520Cybers%25C3%25A4kerhet.pdf&usg=AOvVaw3jdk2yrwZDtkMWSQejPSFx&opi=89978449 [access: 10.09.2023]

27 E.M. Włodyka, *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, ibidem 2022, no. 1, p. 216.

28 M. Karpiuk, *The executive agency as a legal organisational form of implementing cybersecurity tasks*, ibidem 2023, no. 1, p. 58.

Cybertruslen mod Danmark 2023, København 2023.
Dataangrep er blant de største truslene mot Norge. Derfor er kraftsektoren et ettertraktet mål, https://www.tekna.no/kurs/innhold/dataangrep-er-blant-de-storste-truslene-mot-norge.-derfor-er-kraftsektoren-et-ettertraktet-mal/ [access: 11.09.2023].
Dataangrep i Norge: Hackerne kunne gått til cyberangrep på Nato, Forsvaret og Slottet. De valgte norske departementer, „Aftenpoften", https://www.aftenposten.no/norge/i/dwBdWO/dataangrep-i-norge-hackerne-kunne-gaatt-til-cyberangrep-paa-nato-forsvaret-og-slottet-de-valgte-norske-departementer [access: 11.09.2023].
Eurydice-raportti: Suomalaisten aikuisten digiosaaminen on Euroopan kärkipäätä, https://www.oph.fi/fi/uutiset/2022/eurydice-raportti-suomalaisten-aikuisten-digiosaaminen-euroopan-karkipaata [access: 8.09.2023].
Franckiewicz M., *Internett på Island*, https://ts2.space/nn/internett-pa-island/ [access: 11.09.2023].
Gębski M., *Rada Nordycka – regionalna „Unia" na Północy*, 2021, https://www.forum-ekonomiczne.pl/publication/rada-nordycka/ [access: 10.09.2023].
Jensen M.S., *Cyberresiliens, sektorprincip og ansvarsplacering – nordiske erfaringer*, „Internasjonal Politikk" 2019, vol. 77, no. 3.
Jönsson L., *DIGG-rapporten: en lägesrapport om svensk digitalisering*, 2023, https://digiteket.se/inspirationsartikel/digg-rapporten-en-lagesrapport-om-svensk-digitalisering/ [access: 8.09.2023].
Kaczmarek K., *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, no. 1.
Karpiuk M., *The executive agency as a legal organisational form of implementing cybersecurity tasks*, „Cybersecurity and Law" 2023, no. 1.
Karpiuk M., Pizło,W., Kaczmarek, K., *Cybersecurity Management – Current State and Directions of Change*, „International Journal of Legal Studies" 2023, no. 2.
Pohjoismainen ulko- ja turvallisuuspoliittinen yhteistyö, https://um.fi/pohjoismainen-ulko-ja-turvallisuuspoliittinen-yhteistyo [access: 8.09.2023].
Press release of the U.S.–Nordic Leaders' Summit in Helsinki on 13 July 2023, https://www.presidentti.fi/en/press-release/press-release-of-the-u-s-nordic-leaders-summit-in-helsinki-on-13-july-2023/ [access: 8.09.2023].
Radoniewicz F., *Zwalczanie cyberterroryzmu w ramach UE – wybrane aspekty karnomaterialne*, „Cybersecurity and Law" 2019, no. 2.
Redegørelse om Danmarks digitale vækst 2022, København 2022.
The Cooperation Areas, https://www.nordefco.org/The-Cooperation-Areas [access: 8.09.2023].
The Nordic Defence Cooperation (NORDEFECO), https://www.defmin.fi/en/areas_of_expertise/international_defence_cooperation/nordic_defence_cooperation#b67ddad9 [access: 8.09.2023].
Tomala M., *Współpraca międzyparlamentarna Rady Nordyckiej z perspektywy konstruktywizmu*, „Przegląd Sejmowy" 2019, nr 5.
Vildhjärta J., *Pestel-analyysityökalun luominen organisaation kyberturvallisuuden tueksi*, Tornio–Rovaniemi 2023.
Włodyka E.M., *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewniania cyberbezpieczeństwa*, „Cybersecurity and Law" 2022, no. 1.
Wojna dała impuls. Państwa nordyckie rozwijają cyberobronę, https://cyberdefence24.pl/polityka-i-prawo/wojna-dala-impuls-panstwa-nordyckie-rozwijaja-cyberobrone [access: 8.09.2023].

Państwa nordyckie wobec zagrożeń cyfrowych

Streszczenie

Postęp technologiczny i rewolucja cyfrowa sprawiły, że znaczna część aktywności społecznych przeniosła się do sieci. Internet stał się narzędziem, bez którego trudno wyobrazić sobie funkcjonowanie współczesnych państw. Jednocześnie część konfliktów między państwami także przeniosła się do sieci, a państwa o najwyższym stopniu cyfryzacji, do których można zaliczyć państwa nordyckie, stały się celem ataków innych państw lub organizacji.

W artykule autor podjął próbę odpowiedzi na pytanie: W jaki sposób państwa nordyckie i ich społeczeństwa bronią się przed cyberzagrożeniami? Porównał charakterystyki przeprowadzanych przeciwko nim ataków oraz poziomy cyfryzacji społeczeństw.

Słowa kluczowe: współpraca nordycka, cyberzagrożenia, umiejętności cyfrowe, DDoS