NATO PARLIAMENTARY ASSEMBLY

COMMITTEE ON DEMOCRACY AND SECURITY (CDS)

MISSION REPORT*

Virtual visit - Estonia

22 April 2021

098 CDS 21 E | Original: English | 8 June 2021

* This Mission Report is presented for information only and does not represent the official view of the Assembly. This report was prepared by Nathan Robinson Grison, Director of the Committee on Democracy and Security.

I. INTRODUCTION

1. On 22 April, 18 parliamentarians from 14 NATO members and partner countries and the European Parliament participated in a virtual visit of the Committee on Democracy and Security (CDS) to Estonia. The parliamentarians engaged in comprehensive discussions with government, military, academic, and civil society experts on Estonia's experience in:

- building societal resilience to disinformation;
- effectively countering cyberattacks; and
- facilitating practical, direct, and secure interactions between citizens and public institutions through electronic means.

2. The CDS Chairperson, **Angel Tilvar** (Romania) greeted members and thanked the Estonian delegation for welcoming the Committee to Estonia, albeit online. He noted that both disinformation and cyberattacks constitute major security threats to Allied societies. Ill-intentioned actors are increasingly using these hybrid methods of warfare to advance their strategic interests and undermine Allied security and democratic resilience. Estonia's example offers insights about ways for NATO countries to further develop their ability to respond to these challenges.

3. The Head of the Estonian Delegation to the NATO PA, **Oudekki Loone**, welcomed members to the event and discussed the definition and classification of both cyberthreats and disinformation. She added that Estonia has developed best practices in countering these threats and contributes to the development of common approaches against them at the NATO level.

4. The meeting was held under the Chatham House rule. As such, the following report reviews the key themes discussed without attributing any positions or viewpoints to attendees.

II. ESTONIA'S EXPERIENCE IN BUILDING RESILIENCE TO DISINFORMATION

A. THE THREATS FACED BY THE ESTONIAN SOCIETY IN THE INFORMATION SPACE

5. Hostile information activities constitute a major threat for Estonia. Russia has used such activities against the Baltic country as part of its hybrid warfare strategy. Moscow's main objectives in infiltrating and corrupting the local information environment are to shape opinions about Russia, generate societal polarisation, as well as create and exacerbate dissatisfaction with the authorities. Ultimately, Russia's disinformation and propaganda campaigns aim to undermine the legitimacy of the Estonian authorities and the resilience of the Estonian society.

6. Accounting for about 25% of the Estonian population, Russian speakers rely primarily on Russian-language media to access information. They are therefore more exposed to Moscow's disinformation and propaganda. Russia tries to exploit this substantial exposure by spreading disinformation specifically targeting the Russian-speaking minority. However, 30 years after Estonia regained its independence, the Russian-speaking population feels more integrated in the Estonian society, and its media consumption habits are shifting from Russia-based channels to national channels. In 2015, the Estonian Public Broadcasting launched ETV+, Estonia's first public Russian-language free-to-air television channel. Russia is therefore increasingly unable to reach out to and instrumentalise the Russian-speaking minority as it did in 2007.

7. That year, after the Estonian government decided to relocate a monument to Soviet troops from central Tallinn to a nearby military cemetery, Russia launched an intensive disinformation campaign. The campaign, which spanned several months, targeted primarily

the Russian-speaking minority and succeeded in precipitating riots on the streets. It ran alongside a series of cyberattacks, the first known incidence of such an assault being perpetrated by one country against another.

8. Russia has successfully disseminated disinformation in the broader Estonian information space on other occasions. For instance, in 2008, Russian media outlets spread allegations of Estonian involvement in the conflict in Georgia, which were taken at face value by some Estonian media outlets. In the following years, the Estonian media learnt from its mistakes and strengthened its ability to distinguish between fake and real news, to avoid further dissemination of Russian disinformation.

9. Some citizens remain, however, vulnerable to manipulation and susceptible to becoming vehicles for disinformation. Insufficient levels of media and digital literacy magnify the spread of both misinformation (the inadvertent dissemination of inaccurate information) and disinformation. This became particularly evident during the pandemic, as some Estonians contributed to the spread of various conspiracy theories relating to the virus on social media. Russian hostile information actors weaponise the public's confusion and inability to distinguish between truth and falsehood in order to spread their false and harmful narratives among Estonians.

10. Sophisticated tools such as deep fakes have emerged as a cause for concern for authorities around the world, including in Estonia. They do not appear, however, to have become major threats in the information space so far, as solutions to identify and expose them exist. Instead, disinformation and propaganda actors tend to favour less advanced and technical tools, which should therefore be the focus of responses to hostile information activities.

B. ESTONIA'S MULTIFACETED APPROACH TO COMBATTING DISINFORMATION

11. Over the past two decades, Estonia has developed a robust institutional and strategic framework to combat disinformation. This framework has continuously evolved and improved based on the challenges that the country has faced in this field and the lessons it has learnt from them.

12. Psychological defence and strategic communication are cornerstones of Estonia's response to hostile information activities. They form one of the six pillars of Estonia's National Security Concept. Psychological defence refers to efforts to inform the public and raise its awareness about disinformation that aims to undermine the country's constitutional order and societal principles. Strategic communication involves ensuring consistency among all of Estonia's political, economic, and defence messaging and actions and successfully communicating them to the public. Psychological defence and strategic communication complement one another and are essential to neutralising hostile information activities.

13. A dedicated team for strategic communication was created at the Government Office in 2018. The three main pillars of its work are developing situational awareness, improving resilience to hostile information activities, and guaranteeing the efficacy and efficiency of government communications during a crisis.

14. Situational awareness is critical to strategic communication, as it gives decision-makers a comprehensive view of the situation and informs their response to ongoing developments. The Estonian authorities develop their situational awareness through two strands of work. First, they analyse and monitor the information space in Estonia, in Russia, and in select Allies. Second, they undertake research on societal opinions and attitudes among Estonians. While

the focus of situational awareness efforts is typically on security-related matters, it has expanded over the past year to include COVID-19-related issues.

15. Strategic communication and transparency are at the heart of the Estonian authorities' strategy to combat disinformation. Their assessment of the threats posed to the Estonian society is regularly made public. This ensures that the public and the authorities share a common understanding of the disinformation risks faced by the country. The security services publish annual reports on the threats faced by the country, including in the information space, and have demonstrated a willingness to expose the actors behind disinformation campaigns and the methods they use to carry them out, when possible.

16. The Estonian authorities have further developed their ability to communicate effectively with the population during the COVID-19 pandemic. They have established a reserve list of experts from the public and private sectors who are trained in crisis communication. In case of an emergency, they can support the authorities and contribute to their communications efforts.

17. Developing media literacy among the public is crucial to ensure that citizens do not become unwitting propagators of misinformation and disinformation. Estonia has therefore developed innovative solutions to foster resilience to disinformation. The high school curriculum features a compulsory course on media manipulation and places emphasis on teaching students about cyber and information hygiene. The Estonian authorities also organise a national media literacy week and distribute brochures on civil preparedness to the population.

18. Finally, the authorities rely on civil society organisations to support the development of societal resilience against disinformation. Non-governmental organisations are key actors in Estonia's efforts to strengthen its psychological defence capabilities against hostile information activities.

III. ESTONIA'S EXPERTISE IN COUNTERING CYBERTHREATS

A. ESTONIA'S CYBER EXPERIENCE: BACKGROUND AND KEY INFRASTRUCTURE

19. Estonia has become a world leader in developing online solutions and building a digital society since the 1990s. After the country regained its independence in 1991, the authorities promoted information and communications technologies as a driver of both social and economic growth and administrative efficiency. Today, most public services are available online through Estonia's digital infrastructure. In 2015, Estonia even became the first country in the world to introduce e-voting for elections. The way in which the Estonian public embraced e-voting illustrates the success of the digitalisation of the Estonian society: in 2005, 1.9% of voters used digital means to vote; for the Estonian parliament elections in 2019, the percentage of voters using digital means was up to 43%.

20. Estonia's remarkable success in developing a digital society has placed growing responsibilities on the state to ensure the security of all online services. It has also heightened the risk of cyberattacks against the country and increased their potential impact. The most notable such attack occurred in 2007 when, as noted above, Estonia faced the first known coordinated campaign of cyberattacks targeting a nation state.

21. At the time, multiple entities were targeted within Estonia, including banks, media channels, governmental websites, and the websites of political parties. This attack led Estonia to further conceptualise and bolster cyber security on a domestic level. The following year, the country adopted its first national cyber security strategy. The incident also put cyber threats at

the top of the agendas of international organisations such as NATO and led to the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn.

22. A second incident prompted Estonia to further intensify its focus on cybersecurity. In 2017, a researcher from Masaryk University in the Czech Republic discovered a security flaw in the electronic chips of the Estonian e-ID cards, which are used by citizens and residents to access most public services. The flaw affected approximately 800,000 cards issued since 2014, rendering them theoretically vulnerable. In response, Estonia suspended the certificates of the affected e-ID cards and renewed 94% of all existing e-ID cards. The discovery of this flaw and the Estonian reaction to it underlined the importance of information sharing and international cooperation in addressing digital vulnerabilities and countering cyber threats.

23. Today, Estonia's national online services system is a complex organism that is continuously evolving. The government-provided platform operates under a secure architecture and enables government agencies, businesses, and citizens to access the same data exchange environment. The backbone of the Estonian e-society is made up of two components: the abovementioned e-ID cards and the X-Road. The e-ID cards allow residents to prove their identity when traveling, logging into bank accounts, providing digital signatures, voting online, checking medical records, submitting tax claims, using e-prescriptions, etc. The X-Road system is a secure information and data sharing software that ensures interoperability between the different organisations and information systems that provide roughly 3,000 online services to Estonian citizens. Beyond these two key features, other elements are part of the national cybersecurity approach: policy development, education, research, certification systems, standards, crisis management, cybercrime prevention, and military operations all play a role in preventing and responding to cyberthreats.

24. Estonia has developed a comprehensive and robust organisational structure on cyber security. The responsibility for overall cyber security policy coordination lies with the Ministry of Economic Affairs and Communications. Within the Ministry, the Estonian Information Systems Authority is tasked with the development, administration, and protection of the state's information systems. It also responds to cybersecurity incidents through its Computer Emergency Response Team. The Ministry of Defence is in charge of cyber defence in the area of national defence and supervises the work of the Estonian Defence Forces and the Estonian Defence League in this field. The Ministry of the Interior and the Internal Security Service also play a role in preventing, countering, and responding to cyberattacks. An inter-agency entity, the Cyber Security Council of the Security Committee of the Government, ensures efficient coordination between these various government bodies and oversees the implementation of the national cyber security strategy.

B. CURRENT AND FUTURE CYBER CHALLENGES

25. Cyber threats represent a growing and increasingly complex security challenge. In Estonia, over the past three years, the number of cyber incidents reported to the Information System Authority has been rising. At the same time, however, the number of such incidents that had a security impact has not increased.

26. Cyber threats can take many forms, which makes them difficult to counter. Most are related to robot networks (or botnets) which consist of large networks of compromised devices, such as computers or smartphones, connected to the internet and controlled by a third party. Botnets are primarily used by malicious actors to perform distributed denial-of-service attacks or steal data. They can cause considerable damage. There has also been an increase in recent years in phishing attacks, which are fraudulent attempts to gather personal or sensitive

information such as payment details and passwords. The generalisation of teleworking during the COVID-19 pandemic has led to a notable increase in such attacks in 2020-2021.

27. At the global level, the number of actors involved in perpetrating cyberattacks is increasing. Most cyberattacks are carried out by individuals and groups with financial motivations and can therefore be classified as cybercrime. Others derive from state actors, with Russia, North Korea, and China the most frequently cited suspected sources.

28. Over the last decade, cyberattacks have become increasingly sophisticated, which renders countering them more complex. Even well-prepared countries with advanced capabilities can be adversely affected. For example, the SolarWinds attack in 2020 was a complex cyberattack that affected many US state agencies, departments, security services, and corporations. It is still not clear how much information was acquired by the attacker during the incident. A key issue is that attacks are rarely discovered on time: the average time needed to discover a cyber incident is 200 days, and in the SolarWinds case it was close to a year. Protecting information systems represents a significant challenge because the attackers only need to find one way in whereas defending these systems requires protecting all possible entry points.

29. Efforts to counter cyberattacks operate on multiple levels, including education, security measures, whole-of-society approaches, and specific technological solutions such as multi-level authentication and effective log management. Much can be done on the domestic level through robust legal and policy frameworks. International cooperation is, however, crucial as well.

30. International law offers several possible responses to a cyberattack in cases where state responsibility has been established. Countermeasures may be in kind but should be proportional and primarily aimed at stopping the attack. Attributing cyberattacks effectively is, however, notoriously difficult. From an academic perspective there has been clear progress, and countries are more open to discussing the legal and technical layers of attribution and sharing how they have achieved it. Attribution is nevertheless a political issue, and the question of how to respond to attacks remains a subject of debate.

31. Other contemporary challenges relate to trust in technology and technology providers. Individual technical inspections of all hardware and software are simply not possible, meaning countries which rely heavily on digital and cyber solutions must develop and implement rigorous criteria to ensure trust in technology providers. The role of cloud services providers raises additional concerns, especially when they are located in another country. These concerns relate to confidentiality (as the use of new cloud services necessitates revealing information to system operators), data availability (as information stored in data centres may be vulnerable to both physical and cyber incidents), and data integrity (as there is a need to ensure the data is not modified by the cloud service provider or shared with third parties).

C. NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE

32. In 2004, Estonia proposed the establishment of a NATO Centre of Excellence focusing on cyber defence. The NATO CCDCOE was established in 2008, after the 2007 cyberattacks against Estonia highlighted the need for more information sharing and greater cooperation among NATO members and partner countries.

33. The Centre brings together like-minded nations striving for a safer cyber space and increased resilience to threats in the online domain. Twenty-nine member and partner nations have now joined the CCDCOE, with five other countries in the process of joining.

34. The CCDCOE, which is not part of the NATO command structure, carries out the following activities:

- Research: The CCDCOE produces the *Tallinn Manual*, an academic study analysing how existing treaties of international law apply in cyberspace. A follow-up study, the *Tallinn Manual 3.0*, has recently been launched to take account of new developments.

- Training: The CCDCOE runs over 20 courses on topics including strategic executive cyber security, international law, operational planning, and several technical courses.

- Exercises: In mid-April 2021, the CCDCOE hosted its annual *Locked Shields* exercise which has grown to be the largest live-fire cyber defence exercise in the world with more than 30 participating nations. The exercise is premised on building life-like target sets with critical cyber components such as power stations, power grids, air defence, and satellite links. This ensures that defensive teams gain comprehensive experience of how to defend their nations and vital systems in case of a major cyberattack. The *Locked Shields* exercise also fosters cooperation by bringing together military, civilian, academic, government, and industry representatives.

IV. SECURING THE DIGITAL TRANSFORMATION OF THE ESTONIAN SOCIETY

35. As most public services are available online in Estonia, the protection of data is paramount for the country. Large amounts of personal information and data on Estonian citizens must be stored securely. In addition, because non-Estonia-based individuals and companies have the possibility of obtaining e-residency in the country, the authorities must protect these foreign data as well.

36. Estonia has therefore developed a digital infrastructure that is vast and secure, yet flexible and efficient. As mentioned above, the X-Road software lies at the heart of this infrastructure. It is used to exchange data securely between different services. It works according to the once-only principle, which means that only one agency can ask for a particular piece of data from a user. Thus, if one server is hacked, only one type of information will be compromised. This compartmentalisation of the integrated network makes the latter more resilient to cyberthreats.

37. This approach does not only render the X-road software more secure, it also makes it more user-friendly. Citizens only need to enter information into the system, such as a change of address, once to notify all relevant agencies and organisations. The system's user-friendliness and the ubiquity of online services have resulted in a high uptake by Estonians, who, for instance, fill 96% of their tax returns online.

38. The development of digital services has sensitised the population to the importance of data protection. In response, the authorities have taken measures to ensure transparency in the ways in which citizens' personal information and data are used. In particular, the X-road software includes trust measures in the form of a data tracker through which citizens can see which government authority has accessed specific personal data about them in the system and for what reason. This gives Estonians a sense of data ownership and generates accountability and transparency on the part of the authorities.

39. To ensure the continuity of digital public services in case of a major shock affecting Estonia, such as a large-scale cyberattack, natural disaster, or conventional attack on a data centre, the country established a data embassy in 2017 in Luxembourg. It is the first country in the world to open such an embassy. The embassy serves as a back-up site outside Estonia's borders where copies of Estonians' most critical and confidential data are stored. It complements previously existing back-up data storage facilities located on Estonian territory.