

Cyber Security In Estonia 2020

Contents

The Year of Shaping International Law	3
Cyber Security Governance in Estonia	5
Threats and Challenges in Civilian Networks	8
Cybercriminals Keep Us on Our Toes	11
Threats and Challenges to Estonia's National Security	14
Threats and Challenges Around the World: Russian Cyber Threat.	18
Attribution and Deterrence in Cyberspace.	23
The Challenge of 5G Networks: A View From Estonia.	26
NATO CCDCOE Training the Alliance	28
Defending the Nation Needs Steady Planning	32
The EDF Cyber Command: What Is It and What Does It Do?	34
The EDL Cyber Defence Unit: Preparing For The Storm	36
Engaging the Cyber Security Community At Home and Abroad	38
Making I-voting Even More Secure And User-friendly.	43
Protecting Personal Data Becomes An Issue Of Trust	46
EISA: A Collaborative Effort To Boost Estonian Cyber Potential	48

DISCLAIMER:

All chapters express the views of the respective institutions that are identified at the top of each chapter.

For general inquiries and media requests regarding the publication please contact the Estonian Information System Authority at www.ria.ee.

For specific questions regarding topics discussed in each chapter please contact the institutions directly.

The Year of Shaping International Law

KERSTI KALJULAI

President of the Republic of Estonia

If we want cyberspace to become a safe, secure, and stable domain, then malicious cyber activities should have similar consequences as attacks carried out in the 'analogue' world. Part of this deterrent is also clearly stating how international law applies in cyberspace – and this is something where Estonia was able to chip in last year.

Cyberattacks have, for quite a long time, been the weapon of choice for various state, state-backed, and non-state actors in promoting their subversive goals – whether it is stealing money, influencing democratic processes, or just wreaking confusion. One of the reasons is that there is no clear and consensual agreement on how international law and the consequences of breaking these laws apply to cyberattacks and -activities. Indeed, the last couple of years have seen a notable improvement on this issue mainly through states using attribution more actively. To put it bluntly: you still have a pretty good chance of conducting a coordinated, malicious, and devastating cyberattack – and



getting away with it even if the consequences of your activities in the case of conventional attacks or activities would mean a serious breach of international law. Not to mention everything that would come after this in our 'analogue' world — condemnations and resolutions by international organisations, sanctions, travel bans, and other restrictions.

Therefore, creating a clear and agreed understanding on the application of international law *vis-à-vis* cyberspace is not a theoretical and philosophical issue, but at the end of the day, a question of deterring cyberattacks and keeping our digital societies safe and secure. To bring an obvious parallel from the analogue world — international law and con-

ventions have not managed to eliminate wars and use of force as an instrument of international affairs, but they most certainly have limited the number and intensity of conflicts, as everybody is still deterred by the possible consequences of going against the rules-based international order.

The challenge here lies in the fact that international law does stem, among other things, from conventions, agreements, and customs — but first and foremost, it is still only the states themselves who can define and interpret international law in a way that makes academic theories become acclaimed tenets of law and order.

Taking all that into account, I was actually a bit surprised to realise a couple of years ago that Estonia — the world's first digital state, target of the first politically motivated and coordinated cyberattacks back in 2007, and home of the Tallinn Manual on the relations of cyber and international law — was still missing its official positions on this issue. That is why I convened a group of Estonia's best law

and cyber experts to my office back in the autumn of 2018. By the end of that meeting, everybody more or less agreed that — all things considered — Estonia's official positions should indeed be drafted, confirmed by the Government, and publicly introduced.

The Estonian positions themselves (see textbox), introduced at CyCon 2019, are relatively simple, and one could even say — quite habitual. However, they do carry a clear — and now official — understanding of how Estonia perceives this very important issue. As such, these positions are already helping us to further develop and interpret international law in international organisations and forums. As a non-permanent member of the United Nations Security Council, Estonia, among other issues, intends to raise awareness of the threats that emerging cyber risks entail for our societies and security. For example, in March 2020, we raised the issue of cyber security for the first time in the UN Security Council when Estonia, alongside the United States and the United Kingdom, condemned the

**SUMMARY OF ESTONIAN POSITIONS
ON HOW INTERNATIONAL LAW
APPLIES IN CYBERSPACE:**

1. International law applies to state behaviour in cyberspace.
2. States are responsible for their activities in cyberspace.
3. States have to make reasonable efforts to ensure that their territory is not used to adversely affect the rights of other states.
4. States have the right to attribute cyber operations both individually or collectively according to international law.
5. States have the right to react to malicious cyber operations, including using diplomatic measures, countermeasures, and, if necessary, their inherent right of self-defence.

See more: vm.ee/en/cyber-security



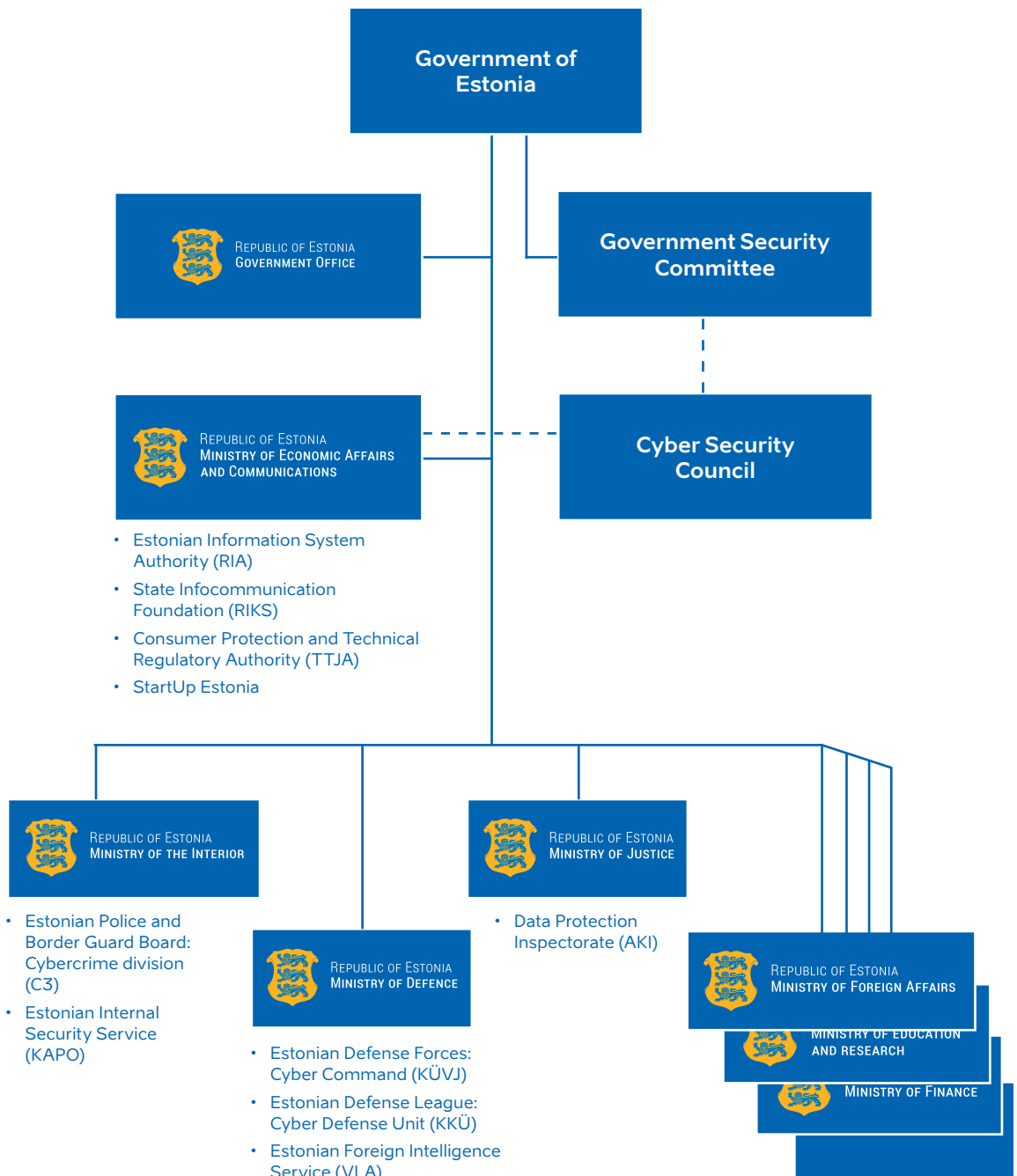
President Kersti Kaljulaid speaking at CyCon conference in 2019 where she presented the Estonian positions on how international law applies in cyberspace.

extensive cyberattacks against Georgia in 2019 and attributed them to Russian military intelligence. There are also two parallel working groups in the UN currently tackling cyber topics and Estonia's official positions are being used to promote discussions in those two groups.

There are a couple of countries — the UK, for example — that have already introduced their official positions in the past couple of years. Since mid-2019, many other nations have also followed suit and introduced or supplemented their positions on the relations of international law and cyberspace — Australia, the Netherlands, and France, to name a few.

It is also true that many actors in the international arena will not share our understanding, or will purposefully remain ambiguous on this issue — that is also one way of creating deterrence. As a small and highly digitised state, Estonia, for one, does not have this kind of luxury. As the first post-war President of Estonia, Lennart Meri, once said: 'International law is the nuclear weapon of a small state'. ■

Cyber Security Governance in Estonia



Cyber security is essentially the management and mitigation of the digital and electronic risks of the information society. This is why cyber security is inextricably linked to the development and management of state information systems and data. The goal is to prevent incidents from happening, which means that cyber security has to be integrated into the life cycles of all communications and information systems. If a cyber security incident or crisis were to occur, the state has to have the capabilities to manage the incidents, investigate the cyber crime, and handle all internal crisis situations.

Government Security Committee

Lead by: The Prime Minister
Members: Ministers of Defence, Economic Affairs and Infrastructure, Foreign Trade and Information Technology, Finance, Foreign Affairs, Interior, and Justice.
Responsibility: Analyses and assesses the national security situation and coordinates the activities of the authorities of executive power with regard to planning, development, and organisation of national defence.

Cyber Security Council

Lead by: Permanent Secretary of the Ministry of Economic Affairs and Communications.
Members: Permanent Secretaries of all relevant ministries and top leadership of relevant agencies.
Responsibility: Coordinates cyber security policy, tracks policy implementation, and the state of cyber security in Estonia.

National Cyber Security Policy Council

Lead by: Director of National Cyber Security.
Members: Cyber security leaders and leading experts from all relevant ministries, state authorities, academia and private sector entities.
Responsibility: Advise on the formulation of national cyber security policy and the development of the field.

Read more at mkm.ee/cyber



REPUBLIC OF ESTONIA
MINISTRY OF ECONOMIC AFFAIRS
AND COMMUNICATIONS

Leading ministry in the area of cyber security. In addition to digital development and cyber security, also in charge of the policies of trade, energy, construction, transport, media services, and other areas.

The Minister of Foreign Trade and Information Technology

The political leader in charge of cyber security in Estonia.

Secretary-General of the Ministry

In charge of departments at the ministry and agencies under its authority.

Deputy Secretary-General for IT and Telecom

In charge of the digital development, national cyber security, and communications in general. Responsible for the cohesion of the state information systems, communications services, and national cyber security.

National Cyber Security Director

In charge of the monitoring, management, coordination and development of cyber security both nationally and internationally. The office is mainly responsible of state-level risk assessment, strategy development, policy formulation and drafting of legislation.

National Cyber Security Policy Council

Cyber Security Strategy Working Group

Other focused and ad-hoc working groups



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Threats and Challenges in Estonian Civilian Networks

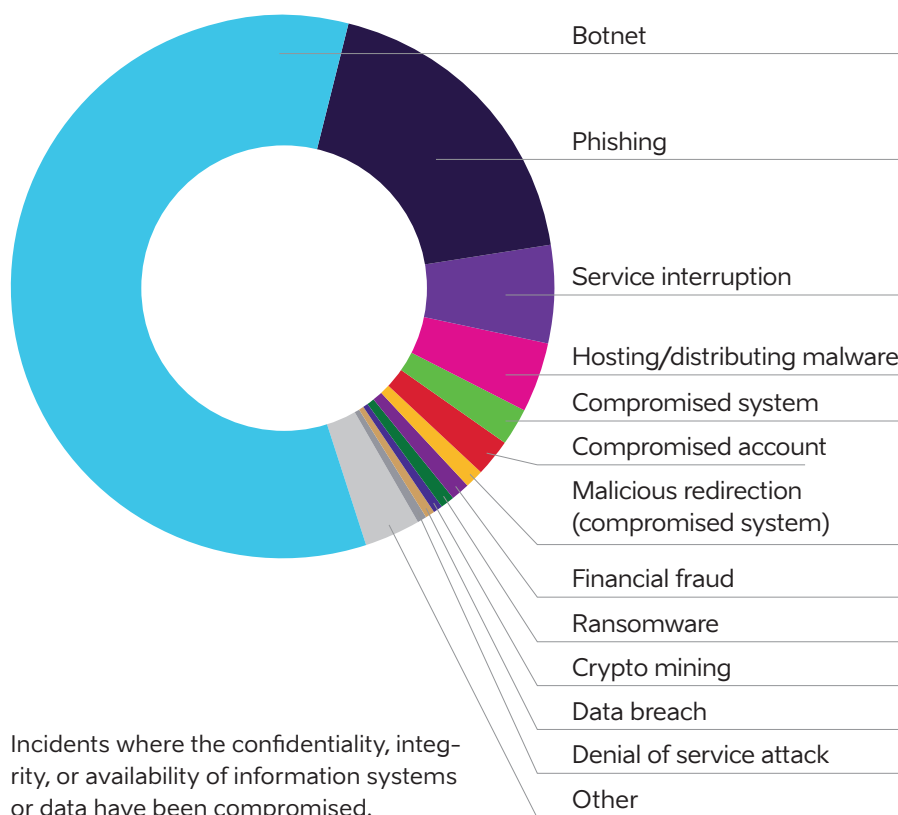
The Estonian Information System Authority (known by the Estonian acronym RIA) is home to CERT-EE, which monitors the Estonian computer network and solves cyber incidents, coordinates the safe implementation of IT infrastructures important for the state, conducts supervision, and raises awareness regarding cyber security. It is also a national contact point for international cooperation in the field of IT security.

CERT-EE is the central point of contact regarding reporting cyber security incidents. Some entities and organisations in Estonia are required to report their incidents to CERT-EE by law (the Cyber Security Act of 2018, which subjects some actors, such as telecommunications providers, critical information infrastructure services, and providers of vital services to a higher standard), but people and companies often choose to inform CERT-EE of their cyber security incidents either to help others or to get assistance themselves.

This constant flow of information regarding cyber incidents, in addition to communication channels with other national and private CSIRT teams, gives CERT-EE and RIA a fairly robust overview of the state of cyber security in civilian networks.

► **A YEAR OF PHISHING.** The year 2019 was a year of phishing for us. The number of incidents concerning phishing campaigns almost doubled compared to the year before. This was mostly because of a large-scale criminal operation attempting to steal money from Estonian internet banks. Up until last year, phishing for Estonian internet banking credentials

INCIDENTS REGISTERED BY CERT-EE IN 2019



and credit card numbers had been mostly futile, since the authentication systems use a form of multi-factor authentication — you get access to your internet bank only if you have a physical ID-card inserted into your computer or if you have access to your phone and know the two PINs required to unlock your personal keys (called Mobile-ID and Smart-ID). The phishing campaigns of 2019 were aimed at that particular part of authentication — luring people into verifying their transactions.

The other phishing trend last year was aimed at stealing e-mail credentials and compromising e-mail accounts. It may seem at first that the goal was simply to access a new set of e-mail addresses that could be spammed with another batch of phishing e-mails. However, the perpetrators behind these campaigns often have a more sophisticated plan in place: to maintain access to the accounts, to identify lucrative e-mail exchanges between business partners, and to interfere in the e-mail thread at the right time to tell a participant in the e-mail thread that their payment for goods should be sent to a different bank account. These account phishing incidents may end up as the initial access points for Business Email Compromise (BEC) schemes.

BOTNETS STILL PLAGUE US

- Over the last couple of years, CERT-EE has constantly reported that compromised systems added to botnets make up the majority of the incidents that we see. This was true in 2019 as well and will continue in 2020. Many of these incidents are still connected to a botnet called Avalanche, which has not been operational since 2016. Another group of compromised systems belong to the Necurs botnet, which was interrupted by Microsoft in March 2020.
- Those systems are just the ones we know about, because law enforcement agencies and international partners inform us of these infected systems when they find out about them. There are many we don't know about. All systems (not just computers and routers, but also webcams and kettles and anything that falls into the category of the Internet-of-Things) that are connected to the Internet are vulnerable to such infections, especially when they are unpatched or when they have their administrative access unchanged.

BUSINESSE-MAIL COMPROMISE RELIES ON THE 'COMPROMISE'.

Multi-factor authentication would help prevent many of these access attempts, but definitely not all of them, since it is sometimes humanly impossible to tell an authentic page from a fake one (and bypassing multi-factor authentication has become more common in the last couple of years). Phishing incidents often do not cross the threshold for 'serious' cyber incidents, which means that there are few resources devoted to figuring out the scope of the breach. This is why we strongly urge organisations to enhance the logging capabilities of their information security teams to understand which data has been extracted, and which partners may be at risk.

We have previously reported that BEC had the biggest impact on Estonian companies and organisations in 2018. In 2019, these types of fraud lost some traction, but were still the most financially devastating for Estonian companies. The losses ranged from 10,000 to over 100,000 euros, which may be business-ending losses for small or medium businesses. In 2019, we also received more information

regarding businesses in other countries that had lost money that they were supposed to send to business partners in Estonia.

CRITICAL SERVICE INTERRUPTIONS REVEAL NEED FOR INVESTMENT.

The year 2019 brought along numerous incidents of interruptions of services that could have had serious consequences. The service of digital prescriptions for medicine that Estonians rely on was interrupted for hours in November due to unscheduled repairs to broken cables, then again offline for hours at a time in December because of legacy software issues. The authentication method called Mobile-ID, which we rely on to access and verify our transactions with the state, was offline for 24 hours in May. This is not a complete list.

Some of those interruptions had short-term impact: people were able to conduct their business later. However, as Estonians rely more and more on digital services for their health and well-being, some service interruptions have a wider impact than others. Fortunately, these interruptions were not caused by malicious activity, but the incidents should serve as a warning to the owners of these services — vulnerable systems may become targets for malicious actors who aim to cause damage. ■



REPUBLIC OF ESTONIA
POLICE AND BORDER GUARD BOARD

Cybercriminals Keep Us on Our Toes

The Estonian Police and Border Guard Board Cybercrime Unit works in cooperation with international partners to detect and investigate cyber-crimes that have affected Estonian citizens and/or is in the Estonian jurisdiction.

► For-profit crime is timeless in its nature — people rob, defraud, and extort others for personal gain. With the development of our society, the means for doing so have changed over time. Cybercrime is just the manifestation of the phenomenon in the context of modern technology. Scams can reach a much broader audience through the medium of the Internet; since finances are digital, it makes much more sense to infiltrate bank accounts rather than the physical establishments, and extorting people by encrypting their files is emotionally much less straining than, for example, kidnapping.

In essence, criminals are still exploiting the same human weaknesses, like greed, optimism, or carelessness they always have, with the difference that the digital sphere is much more alien to most people than the physical world. This means that we have not yet learned to be as cautious on the Internet as we are on the street, but also that we have not learned to notice the important environmental cues that help us avoid danger in the real world.

In this sense, talking about specific new vulnerabilities or malware strings is less important, since the successfulness of using them boils down to how informed and vigilant the target is. Your code might be able to do horrendous things to the security or integrity of a person's data, but only if they click the link you sent them or run the macros you embedded in the attachment, right?

The same goes for safety standards — providing patches for services helps prevent the exploitation of vulnerabilities, but only if people actually update their systems. Using strong passwords for platforms makes it harder to crack them, but only if we do not go and insert them on a fraudulent imitation of the webpage we actually wanted to visit. The latter also applies to two-factor authentication, which helps protect your account in case (or rather when) there happens to be a leak of user passwords, but only if you pay attention and do not authenticate the login of the criminal using your leaked password.

 **ONLINE BANKING SCHEME.** In 2019 we saw the emergence of attacks targeting people's Smart-IDs, which justifiably called into question the safety of Estonia's digital state. In reality, the system is intact and secure, but the users are still vulnerable. The reason why some of the attacks on the Smart-ID were successful, regardless of the two-factor authentication, is that people did not pay attention to the webpage's URL that was sent to them by the fraudster with the pretext of the service provider requiring their authentication. The investigation into the attacks is still ongoing, but the lesson that can already be learned is that no application, institution, or regulation can contribute to the prevention of cybercrime as much as the users understanding the system they are interacting with and being aware of the signs of danger when roaming the wide digital plains of the Internet.

As a response to these kinds of attacks, we are actively cooperating with relevant institutions and CERT-EE with the goal of disrupting the ongoing attacks and collecting relevant evidence. Especially in cybercrime, it is important to have great communication between public and private entities, both in Estonia and internationally, in order to have an appropriate reaction to these kinds of cases.

Although not all cybercrime is motivated by financial gain, today, its most widespread and visible forms are mostly driven by the criminal's desire to earn a profit. This can be achieved through directly targeting a person with a phishing email, trying to steal their logins through a fake webpage, or infecting their machine with malware, or even by enabling other criminals to do so.

The latter can be considered the root of the problem — the underground economy of cybercrime is well developed and widespread, which enables more and more people to become involved in criminal activities. The marketplace has a high level of specialisation with competing vendors offering a variety of goods and services necessary for launching cyberattacks against an array of targets. This means that anybody with a Bitcoin wallet can purchase dumps of compromised accounts, bullet-proof hosting services, malware code, crypters, order DDoS attacks, and so on. In other words, the entry barrier for becoming a cybercriminal has drastically decreased in terms of the skills and resources required, while the rewards are constantly increasing thanks to the continued digitalisation of our society.



► **AIM TO DISRUPT.** From the perspective of law enforcement, it is of course important to find the people using these goods and services against our citizens, but in order to fight cybercrime as a phenomenon, we must seek to disrupt the systems that enable it. Reactively finding and prosecuting individual offenders is an important deterrent, but removing a vendor or an entire marketplace will stop another from taking their place. As law enforcement, we will have to continue to identify and uncover the hidden structures that do not abide by the laws we have set, even if they now exist on the new, non-physical frontier.

As long as our personal lives, business, and state services are digital, there will be an incentive for criminals to go cyber. In the upcoming year, we can expect new malware to be developed, new vulnerabilities to be discovered, and innovative stories to scam people to let their guard down. These are a constant and inevitable part of our modern reality. In order to mitigate their negative effects on us, we have to learn to understand the new environment that encompasses our lives. ■



REPUBLIC OF ESTONIA
INTERNAL SECURITY SERVICE

Threats and Challenges to Estonia's National Security

Estonian Internal Security Police detects and prevents attacks threatening national security, committed either by other countries or terrorist organisations.

This is an excerpt from the 2020 edition of the the annual review of the Internal Security Service available for download at kapo.ee.

In cyber security, KAPO's job is to detect and respond to cyberattacks. Foreign countries use their offensive capabilities consistently, purposefully and at a high technical level. Internationally, this type of cyberthreat is known as the advanced persistent threat (APT).

► **DANGEROUS PHISHING EMAILS.** With regard to cyberattacks of foreign origin or which threaten national security, we must once again address the danger of phishing emails. Last year, malware hidden in fake emails was used to access the data of many Estonian individuals and institutions. While phishing scams pose a threat to the general public, attempts by foreign intelligence services have a narrower range of persons of interest: diplomats, politicians, scientists in certain fields, people involved in military and national security — in other words, anyone who could have access to information that is of interest to the special services.

Last year, the private email accounts of such individuals continued to be targeted. For example, a person in Estonia who uses a hotmail.com account was sent a highly plausible fake email, luring the recipient to click on a link in the message and enter their password on a website very

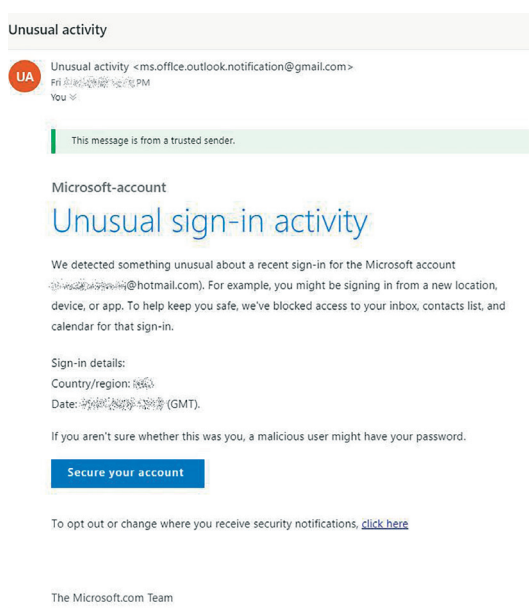
similar to Hotmail but controlled by the attacker (see example).

Attempts targeting private email accounts were also made with mail.ee accounts (see description below). It is probably self-evident that the contents of a private account of a person who has access to sensitive information provide necessary information to hostile intelligence services even when they do not include anything work-related. A private email account is a private matter and the user is responsible for its security. Although phishing emails generated by foreign services look very much like genuine messages, they are not incomprehensibly hightech.

If the user is alert and aware of security issues, they can avoid being compromised by such emails or detect any security breaches that have already occurred. Below are our suggestions for raising security awareness.

In addition to phishing emails directed at private email accounts, we also identified attempts by national-level attackers to access institutions' email services and thereby also their computer networks. For example, the following phishing email about Ukraine was sent to Estonian state authorities (see example). This is a national-level offensive campaign known in the cyber security community as the Gamaredon advanced persistent threat (APT) group.

A phishing email was also used to try to gain access to some email accounts connected to the University of Tartu. This was probably a campaign organised at the behest of the Iranian government by an actor also known as the Silent Librarian or the Mabna Institute. Thanks to its proficiency, the University of Tartu was able to identify the attack and prevent any major damage.



► **SECURITY VULNERABILITY SCANS.** The cyber operations of foreign special services use many of the same methods as cybercriminals or malicious activists. Scanning the services and devices of a prominent online target for security vulnerabilities is one of these. Notable vulnerabilities with the highest and broadest impact are VPN firewall weaknesses (CVE-2018-13379 — Fortigate and CVE-2019-19781). Worldwide, 500,000 devices are vulnerable and known to be potential targets for an advanced persistent threat. Attackers operate intensively under the cover of other noise. Ongoing campaigns have also identified vulnerability patching to secure an exclusive online presence. It is therefore advisable, especially for those responsible for security, not to rely solely on a vulnerability checking tool, but also to investigate the logs for a possible attack.

► **THE SERVICE PROVIDER'S IMPORTANCE FOR ENSURING SECURITY.** Private individuals, businesses and institutions have to choose a service provider for using digital services, be it a free personal email account (e.g. online.ee, mail.ee, gmail.com) or a data hosting and management service (email, files, website) for business clients.

For critical and restricted data, the state assesses and manages the related risks. We encourage all individuals, businesses and institutions to do

the same. Often, there are no good options in this regard, but in any case, it is strongly recommended to find out in which country the data will eventually be hosted and how security is ensured, and to implement reasonable security restrictions. We know from experience that businesses and research institutions are often unaware that their data could be of interest to foreign intelligence services working in the economic interests of their country.

RECOMMENDATIONS FOR CHOOSING EMAIL AND OTHER SERVICE PROVIDERS AND SETTING UP ACCOUNTS

- Find out in which country the data of the email or other service are stored and in which country the (parent) company is located or registered.
- Choose a service provider that stores data and is located in a country that respects people's rights and privacy.
- Choose a service provider with various methods for ensuring security: two-step authentication, displaying the IP addresses of the last log-ins, allowing/restricting logging-in with IMAP and POP3, and linking to a specific device.
- Every now and then, review the IP addresses used for logging in, and check whether the IP-WHOIS data corresponds to the IP you use at home, at work etc.
- Every now and then, check whether your emails have been redirected to other email addresses, or which other email addresses are linked to your account.
- If you see a news story about a leak of email user data connected to Estonia, check whether it is relevant to your email account, and if so, change your password or authentication method.

► **CRITICAL SECURITY VULNERABILITY IN THE APPLICATION OF FREE EMAIL PROVIDER MAIL.EE.**

An as-yet-unidentified critical security vulnerability in the mail.ee application, which is extensively used by people in Estonia, was exploited, allowing the attacker to launch a malicious software code on the target's account. Among other things, the attackers were able to redirect to themselves all emails sent to a mail.ee account. Specifically, when the target opened an email sent by the attackers (see example below), this triggered a malicious code contained in the message, which set up email forwarding. From the moment the email with the malicious code was opened, all of the emails sent to the target were redirected to an email account controlled by the attacker.

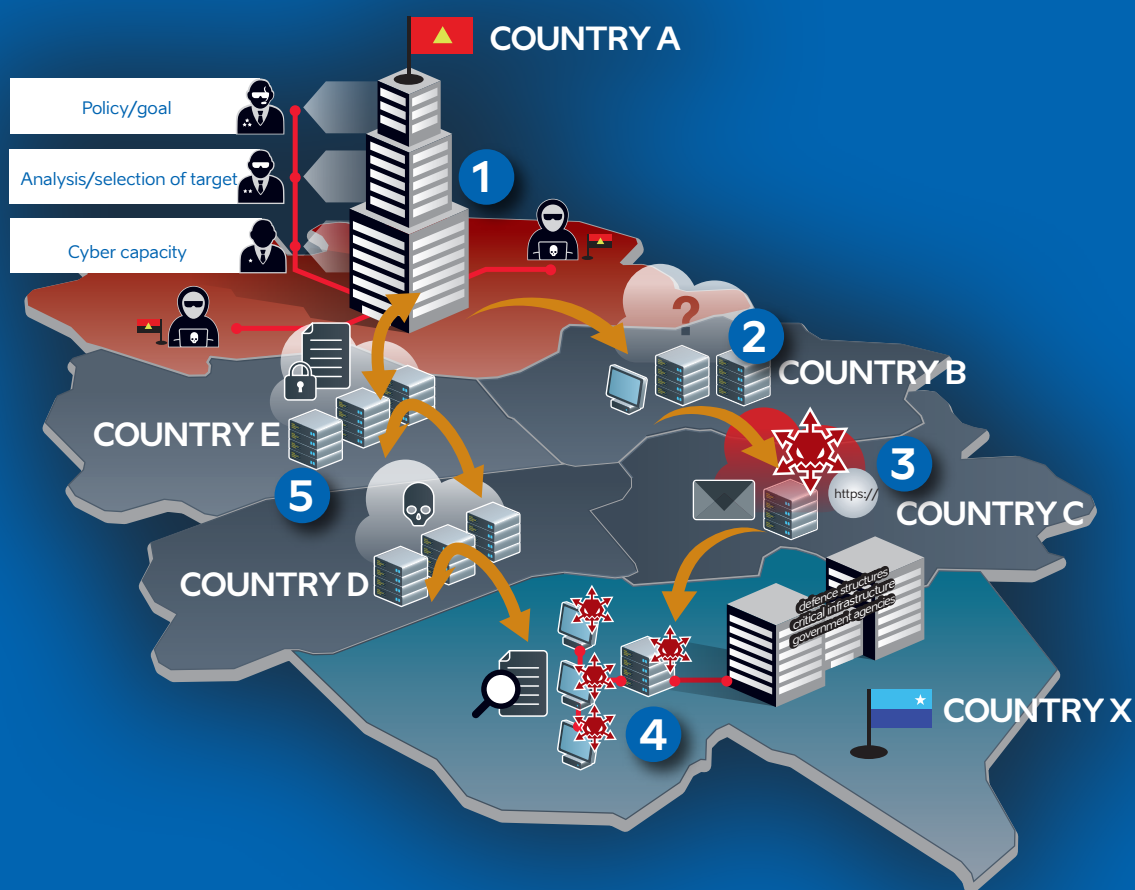
We wish to emphasise that simply opening the email message was enough: the code was triggered without having to

open an attachment or clicking on a link in the message. Afterwards, the user's email settings showed the mail forwarding (see screenshot below). Unfortunately, not many users regularly check their email account settings.

The most important aspect of the case in question is that, as a result of efficient action by the Estonian Information System Authority (CERT-EE) and the owner of mail.ee, the vulnerability was removed and the circumstances were identified. Importantly, this vulnerability was only exploited with regard to a small number of email accounts belonging to persons of interest to a foreign country. The general public and users of mail.ee need not worry. ■

A cyberattack threatening national security is characterised by a complex scrambling of sources:

- a) Use of services allowing for anonymity (registration of servers using false data);
- b) Use of services allowing for encryption (VPNs);
- c) Anonymous means of payment — difficulty in following the money trail;
- d) Infrastructure in various countries and legal environments.



SCHEME OF AN APT ATTACK

1. Selection of target (government agencies, defence structures, services of critical importance)
2. Infrastructure enabling anonymity (springboards)
3. Tactics for delivering malware to the target (taking over an email account, web link, etc.)
4. Infection of the computer network of the target and mapping the information in it
5. Two-sided data transfer to manage the malware, steal information or freeze the system



VÄLISLUUREAMET
Estonian Foreign Intelligence Service

Threats and Challenges Around the World: Russian Cyber Threat

Estonian Foreign Intelligence Service (EFIS) collects, analyses and reports information on Estonia's external security threats. EFIS is responsible for the security of the state's classified networks and carries out counterintelligence for the protection of Estonian diplomats and military personnel posted abroad. EFIS also performs the function of the National Security Authority, being responsible for the protection of foreign classified information.

This is an excerpt from the fifth edition of the Estonian Foreign Intelligence Service's annual report, "International Security and Estonia" which was published February 12th, 2020 and is available for download at valisluureamet.ee.

▶ Cyber operations are an effective means for Russia to achieve its political goals. They are affordable in terms of people, time and financial resources, and allow Russia to operate below the threshold of armed conflict. The targets of Russian cyber operations have changed little through the years – the target countries are mostly the same, while the range of targeted sectors has expanded over time. The strategic objectives of the operations – projecting the image of a superpower and maintaining internal stability – also remain unchanged. What changes, however, is the methods used to perform the cyber operations, which is why consistent enhancement of cyber security is crucial.

Russia has been conducting cyber operations against Western democracies since the 1990s. At first, the operations primarily targeted the military sector, but the range of targets has gradually expanded. Russia uses cyber operations to steal information, but also to undermine

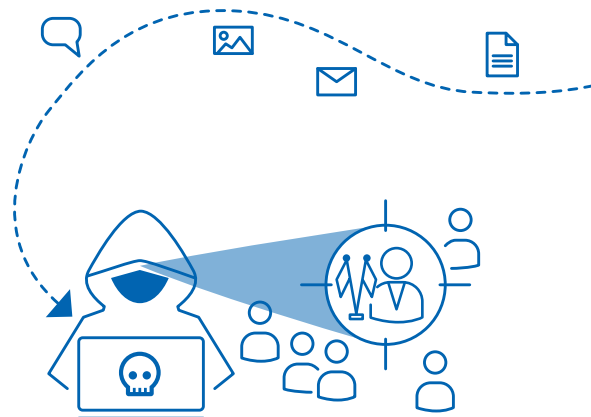
unity in countries, exert influence (for example, creating and fuelling divisions to obstruct political processes), and punish decisions unfavourable for Russia (for example, bans on Russian athletes have been followed by attacks against international sports organisations).

Russia's cyber operations have been successful and, to date, have not been sanctioned enough by the West to force Russia to abandon them. As Russia has received the signal that cyber operations are justifying themselves, these operations will continue to be a security threat, to Estonia among others.

In 2019, Russian cyber operations were revealed that have been going on undiscovered for years, and there are likely to be more. In addition to their continuity, Russia's cyber operations are characterised by the tendency to exploit situations as they arise — as security vulnerabilities become public, the Russians are eager to exploit these immediately against their existing targets. For example, only a month after a security vulnerability was announced in February 2019, Russian cyber actors attempted to exploit it in an operation against an international organisation. This case demonstrates again how important it is to constantly update the software of your IT systems.

WATERING HOLE ATTACK – A METHOD WIDELY USED BY RUSSIAN CYBER ACTORS

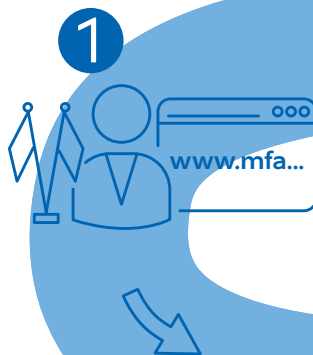
Cyber attackers are looking for the weakest link to achieve their goals — everyone is a potential target. Russian cyber groups may target, for example, the support teams of high-ranking officials or executives (accountants, secretaries, personal assistants, chauffeurs, registrars, etc.). Online devices (computers, routers, smartphones etc.) with low or insufficient levels of cyber security are easy to attack and can unsuspectingly become part of the Russian cyber-attack infrastructure. Russian cyber attackers continually and automatically map devices that are connected to the internet and either have software that is not up to date or are publicly accessible. Having identified such a device, an attacker is likely to compromise it and start exploiting it in their cyber operation.



The attacker is targeting a diplomat from country X to infect their device with malware.

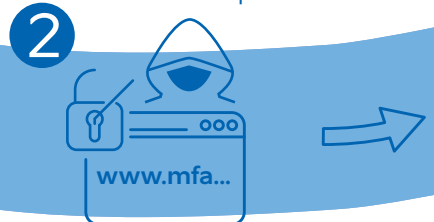
Mapping

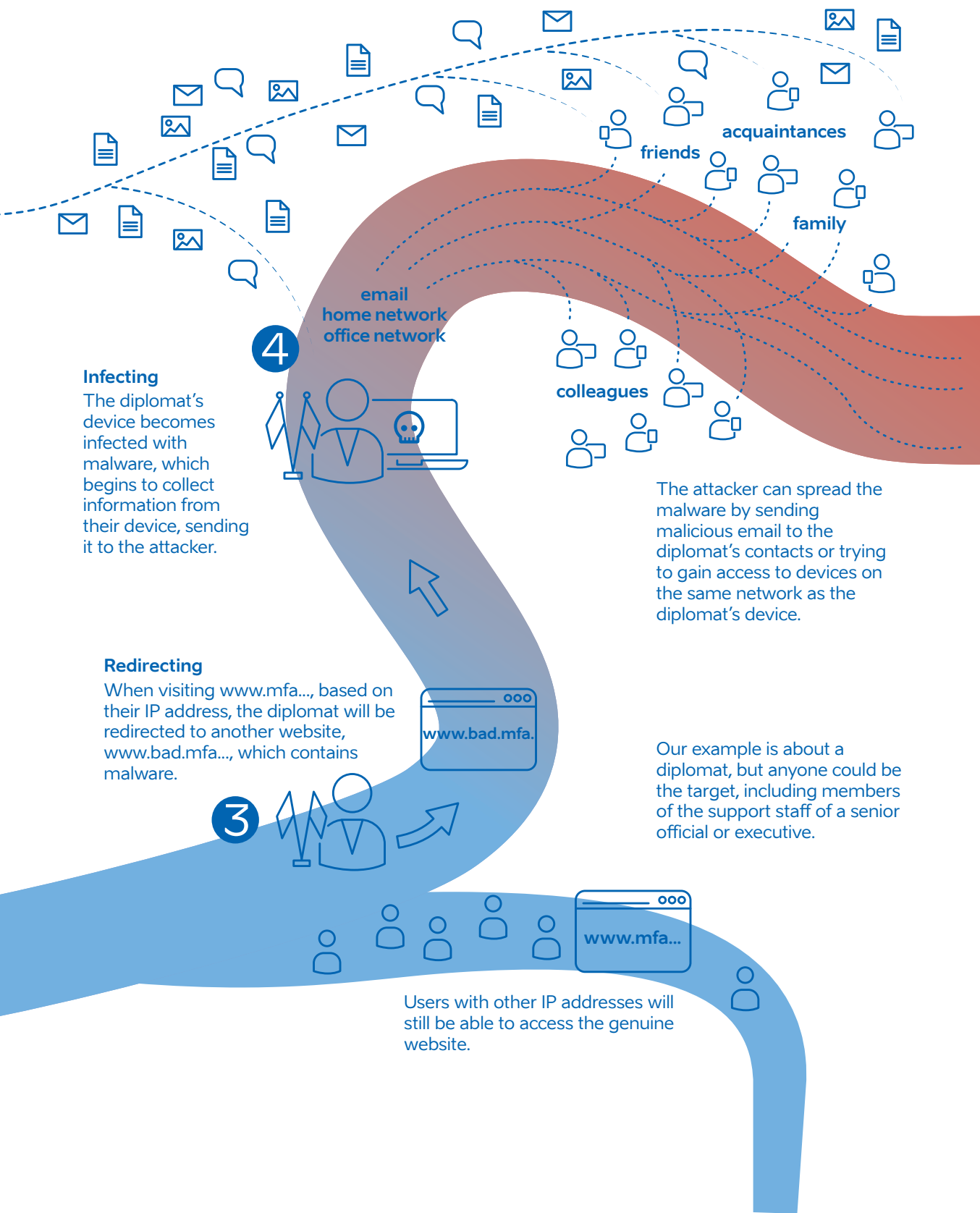
The attacker maps the websites visited by the diplomat and discovers a security vulnerability in the web content management system of one of the sites because the system has not been updated — a foreign ministry website, [www.mfa...](#)



Compromising

By exploiting the security vulnerability, the attacker breaks into the [www.mfa...](#) website and compromises it.





Infesting

The diplomat's device becomes infected with malware, which begins to collect information from their device, sending it to the attacker.

4

email
home network
office network

colleagues

friends

acquaintances

family

The attacker can spread the malware by sending malicious email to the diplomat's contacts or trying to gain access to devices on the same network as the diplomat's device.

Redirecting

When visiting www.mfa..., based on their IP address, the diplomat will be redirected to another website, www.bad.mfa..., which contains malware.

3

www.bad.mfa...

www.mfa...

Our example is about a diplomat, but anyone could be the target, including members of the support staff of a senior official or executive.

Users with other IP addresses will still be able to access the genuine website.

► Russia conducts cyber operations against international institutions mainly to steal sensitive information on what political positions countries hold, which countries can be influenced in directions suitable for Russia, as well as how and whom to target with their narratives in information operations. International institutions are more vulnerable to information leakage, as they use shared systems for the exchange of information between member states with different levels of cyber security. Russia prefers to target states and institutions that have a low level of cyber security and possess sensitive information of another country due to membership in an international organisation.

In the summer of 2019, the European Union External Action Service identified leaks in the information systems of its Moscow delegation, which were traced back to February 2017.

Russia intervened in Western elections in 2019 and is likely to do so again in 2020. This year, for example, Russia's focus will certainly be on the US presidential and Georgian parliamentary elections. The main goal is to ensure a more beneficial election result for Russia by favouring Russian-friendly candidates or those who have the most divisive influence in the West. Moreover, Russia wants to show that the West is failing to hold fair elections, which is an opportunity to divert attention away from Russia's own problems and use the well-worn rhetoric of Western double standards.

The Western military sector has been the target of Russian cyber operations since the very beginning. The main purpose is to obtain a state secret revealing the military plans or capabilities of Western powers. For example, a probable target for the Russian cyber actors is the US-led exercise "Defender Europe 20", which takes place in Europe in May–April 2020.

► Cyber attackers are looking for the weakest link to achieve their goals – everyone is a potential target. Russian cyber groups may target, for example, the support teams of high-ranking officials or executives (accountants, secretaries, personal assistants, chauffeurs, registrars, etc.). Online devices (computers, routers, smartphones and others) with low or insufficient levels of cyber security are easy to attack and can unsuspectingly become part of the Russian cyber-attack infrastructure. Russian cyber attackers continually and automatically map devices that are connected to the internet and either have software that is not up to date or are publicly accessible. Having identified such a device, an attacker is likely to compromise it and start using it in their cyber operation.

In the previous pages is a description of one common method used by Russian cyber groups to infect a target with malware with the purpose of stealing sensitive information. Russia is actively using cyber operations as a political tool. As a result, the targets of Russian foreign politics and cyber operations may overlap. Attackers get to their targets through people close to the target who have low cyber security and limited ability to detect cyber attacks. As long as the potential benefits outweigh the consequences, Russia is very likely to continue its use of cyber operations. ■



REPUBLIC OF ESTONIA
MINISTRY OF FOREIGN AFFAIRS

Attribution and Deterrence in Cyberspace

The Ministry of Foreign Affairs promotes Estonia's interests in the world, develops bilateral and multilateral relations with other countries, and contributes to the joint activities agreed upon in international organisations in order to promote the development of a free and secure cyberspace.

► The year 2019 marked a turning point in Estonia's activities regarding deterrence of cyber operations after the Government of Estonia adopted the country's first attribution guidelines on 24 January. These guidelines established a working group of all relevant ministries and authorities for sharing information on cyber operations and making decisions on possible response options. The working group will be focusing on cyber operations that have targeted either Estonia or our allies and partner countries around the world.

The working group will be assessing each cyber operation individually and on a case-by-case basis, by taking into account its effects on our society as a whole. It is necessary to send a message that harmful cyber operations are not part of acceptable state behaviour and can constitute an internationally wrongful act. Estonia welcomes the efforts that many states have made over the recent years in moving towards a coordinated attribution coalition.

Over the last five years, the world has experienced global and regional cyber operations that pose a threat to the stability of our economies and democratic institutions. These operations have gradually increased in their frequency and severity. This is the primary reason why it has become more important for countries to 'name and shame' persons or

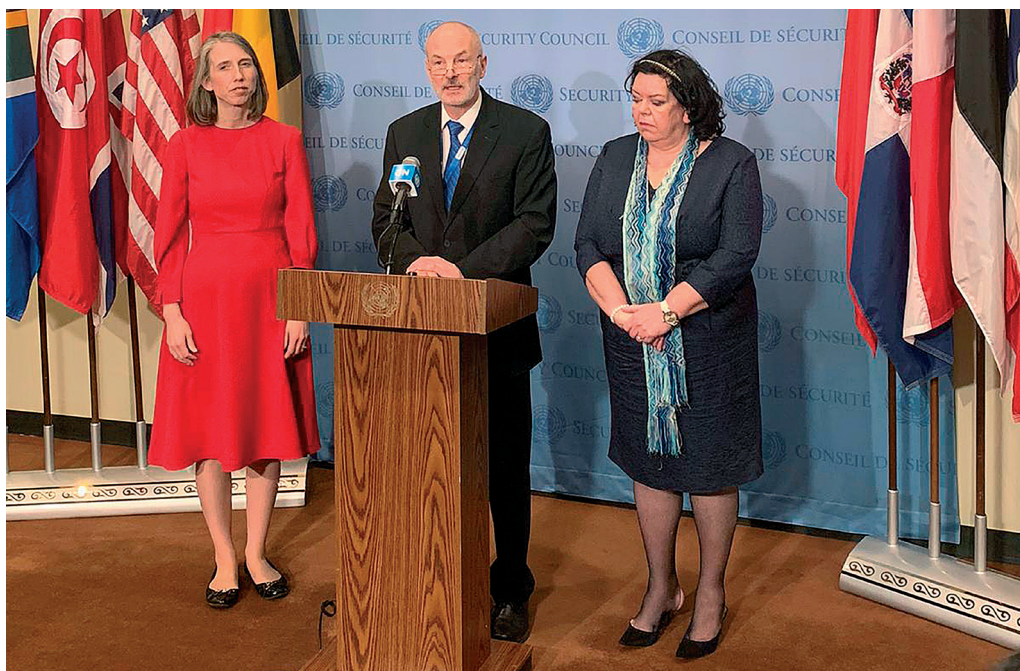
entities behind a cyber operation in order to show that these actors will be facing proportional consequences. Public attribution and messaging are tools for deterring and responding to such behaviour, but also for raising wider awareness in our societies. Public attribution also allows states to send clear messages and shape expectations that malicious cyber operations will not be tolerated, and warn the general public of the seriousness of cyberspace intrusions.

In 2018, Estonia supported the like-minded attribution of operations against multiple organisations, including the Organisation for the Prohibition of Chemical Weapons, to NotPetya, Wannacry, and GU/GRU. One of the most recent public attributions took place in December 2018, when Estonia supported the public attribution of the operation Cloudhopper to APT 10 that works for the Chinese Government.

It is widely believed that public attribution is more effective when conducted in a coordinated manner — or in a coalition. The regional frameworks for coordinated public attribution were strengthened in 2019 to allow states to give a more coordinated response to malicious cyber operations. In 2017, the European Union adopted the first-ever framework on joint EU response to malicious cyber activities (cyber diplomacy toolbox). Estonia has been a long-time supporter of the implementation of measures in the EU cyber diplomacy toolbox that includes a collection of possible responses to malicious cyber activities targeting the organisation itself, one of its member states, or a partner country. The response options could vary from public statements and démarches through diplomatic channels up to the level of restrictive measures, such as asset freezes and travel bans on persons and entities that have launched cyber-attacks. The EU adopted its first restrictive measures in May 2019.

Estonia is a supporter of attribution of malicious cyber operations and using collective measures where possible. When confronted with cyber operations, states have the right to respond in accordance with the existing international law. States have globally agreed upon the fact that international law applies to a state's conduct in cyberspace. This is stated in the 2013 and 2015 reports of the UN Group of Governmental Experts (GGE), endorsed by the UN General Assembly. The UN Charter, international humanitarian law, customary international law, and human rights law have been guiding state behaviour in all other domains, and the interaction between these instruments and state conduct in cyberspace continued and will continue to be strengthened in 2019 and over the years to come.

 **UNITED NATIONS AND CYBER NORMS.** Over the last decade, activities conducted in cyberspace have become a substantive part of the work in the UN First and Third Committees as well as in various other UN bodies and organisations. Since 2009, Estonia has been taking part in the work conducted by the UN GGE — so too in 2019, marking the start of the sixth GGE (2019–2021). Additionally, Estonia took active part in the work of the Open-Ended Working Group (OEWG), which, for the first time, created a platform for all 193 states of the UN to participate in open discussions on emerging and existing threats, international



In March 2020, Estonia raised the issue of cyber security for the first time in the UN Security Council, where we condemned the extensive cyberattacks against Georgia in 2019 and attributed them to Russian military intelligence.

law, norms, confidence-building measures, capacity-building, and institutional dialogue within the UN. Participating in these two First Committee working groups will also continue in the upcoming years, with the need to find a complementary approach between the two groups and making sure that the outcomes of the 2010, 2013, and 2015 UN GGE reports will continue to be the basis of state conduct in the future.

In 2019, the Estonian Ministry of Foreign Affairs analysed the policy and legislative updates that Estonia has made over the last five years that support the implementation of the voluntary and non-binding norms of the UN GGE 2015 report. At the end of 2019, the Estonian Ministry of Foreign Affairs held consultations with the private sector and academia on how these global norms have been used and how could they be better used to advance our national cyber security.

The Estonian State Information System Authority as well as other government institutions have played a key role in contributing to the implementation efforts of each of the eleven norms that range from international cooperation to attribution. In addition to the UN cyber norms process, regional organisations also engage in the cyber confidence building process. The OSCE — where Estonia is an active member — has developed and continues to operationalise confidence-building and transparency measures that are intended to enhance the predictability of states' behaviour in cyberspace. ■



REPUBLIC OF ESTONIA
MINISTRY OF ECONOMIC AFFAIRS
AND COMMUNICATIONS

The Challenge of 5G Networks: A View From Estonia

The Ministry of Economic Affairs and Communications (MKM) is the leading ministry in the area of cyber security. In addition to digital development and cyber security, it is also in charge of the policies of trade, energy, construction, transport, media services, and other areas.

► In 2019, the issue of Fifth Generation (5G) networks captivated governments around the world. The technology in question will, in the coming years, revolutionise the digital economy and society. Worldwide 5G revenues are estimated at 225 billion euros in 2025. So far, both the thought process and the simultaneous debate have been dominated not only by technical questions, but also by different security concerns. Why? Because one of the companies most capable of delivering the relevant technology — Huawei — is in many quarters not seen as an independent tech giant, but an entity controlled by the Chinese government. A key ally of Estonia, the United States, has called Huawei 'a Trojan horse for Chinese intelligence services'. Many Western intelligences services, including Estonia's, share those concerns. It is believed that Beijing is out to create, over a longer time period and step-by-step, dependencies in other states. With a Chinese company that is accountable to the Chinese government supplying the equipment for 5G networks, all the concerns would be amplified. For example, could 5G, which is enabled via a Huawei-built network, be turned off if a country does not play ball?

Estonia, as an extremely digitalised country, is indeed very dependent on information and communications systems. The relevant infrastructure is of critical importance for the functioning of the government and for the

lives our citizens have become used to living. Because of a less centralised architecture, 5G networks offer more potential entry points for attackers.

In these circumstances, the functioning of the digital nation that Estonia has become to view herself as will rest solely on the reliability of the technology provider. This is because the producer is really the only one with all the information about the capabilities, including the possible so-called backdoors of its hardware and software. Not all companies are deemed equally trustworthy in this context. The US banned the use of Huawei network equipment back in 2012. In 2019, countries like Australia and New Zealand followed suit. But in the European Union, the relevant market share of Huawei is over 50% on average. Because of that, since March 2019, the European Union has been trying to coordinate the actions of its Member States on 5G network security.

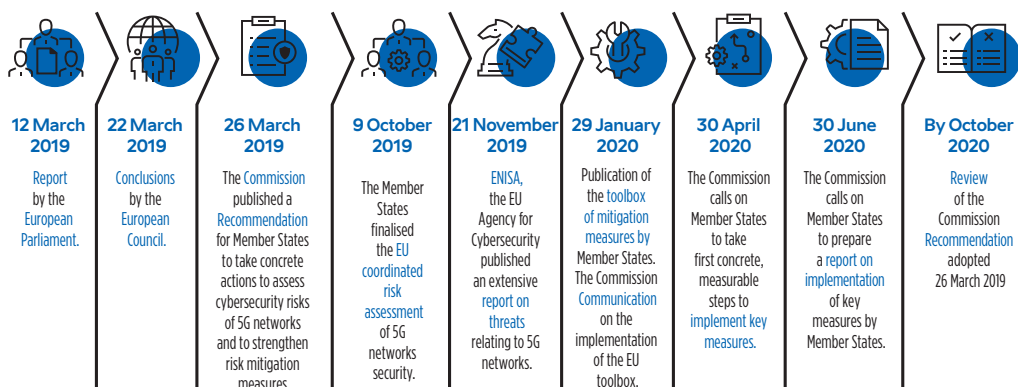
▶ To that end, a special expert group was set up by the European Commission. In October, this group published a coordinated 5G risk assessment. This document focused on the novelty, threats, threat actors, assets, vulnerabilities, and risk scenarios of 5G and deemed as the biggest potential threat the companies that could be influenced by non-EU states with cyber-offensive capabilities. In January 2020, a toolbox of possible measures followed.

This document lists mitigation possibilities for the identified risks and proposes a set of strategic and technical measures to be taken. Among those are relevant legislative measures, security-related requirements, and the recommendation to diversify network component suppliers in order to avoid or limit dependence on one vendor. Work on this will continue in Brussels in the course of this year.

In Estonia, legislation to ensure minimisation of those risks has already been initiated. To ensure high quality and to avoid possible cyberattacks or political manipulation, telecommunications companies will be required to consult and coordinate with the government with regard to any new technology they plan to introduce to electronic communications networks. Once implemented, this will minimise security threats and guarantee the reliability of the future services on offer. ■

EU 5G Cyber Security coordinated approach timeline from the European Commission factsheet.

Timeline





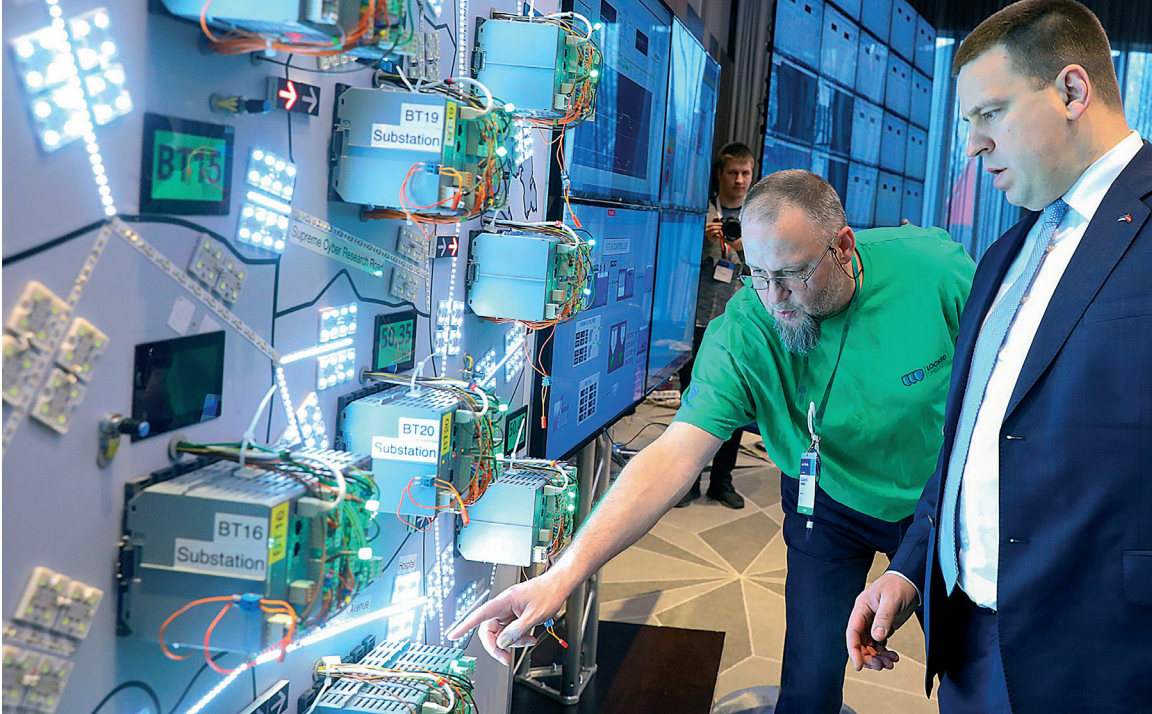
NATO CCDCOE – Training the Alliance

The NATO Cooperative Cyber Defence Centre of Excellence is a multinational cyber defence hub that supports member states and NATO with unique interdisciplinary expertise in the field of cyber defence research, training, and exercises covering the focus areas of technology, strategy, operations, and law.

▶ The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), based in Estonia, is a NATO-accredited cyber defence hub offering a unique interdisciplinary approach to the most relevant issues in cyber defence. The heart of the Centre is a diverse group of international experts from military, government, academia, and industry. To date, the CCDCOE has brought together 25 nations as its members, among them 22 NATO Allies and many more on the path to joining.

The cyber domain is expected to evolve rapidly in the military context. Among the research topics that the CCDCOE experts are currently working on is the analysis of autonomous features of cyber operations, digital forensics, protection of critical infrastructure, cyber command and control, cyber deterrence, cyber effects in battlefield and attribution. From a technological perspective, the crossover of artificial intelligence (AI) and rollout of 5G networks will inspire new technologies that we might not even be aware of now – this is something to keep an eye on.

In twelve years since its establishment in 2008, the CCDCOE has earned recognition for its unique flagships – the world's largest and most complex international live-fire cyber defence exercise (called the Locked Shields), international conference and community-building event CyCon, and Tallinn Manual 2.0, the most comprehensive analysis on how international law applies to cyber operations.



▶ **CYBER DEFENCE EXERCISES.** The Centre has world-class competence in conducting large-scale cyber exercises on the technical as well as strategic level and how to combine them. Locked Shields, organised by CCDCOE since 2010, is the largest and most complex international live-fire cyber defence exercise in the world. More than 1,500 cyber experts from 30 nations took part in Locked Shields 2019. In addition to new critical infrastructure components, it also included a strategic and legal game, enabling participating nations to engage the entire chain of command in solving a large-scale cyber incident. Unfortunately, due to the coronavirus pandemic, Locked Shields 2020 had to be cancelled, nevertheless, work on Locked Shields 2021 has already started.

Prime Minister Jüri Ratas visiting the Locked Shields exercise in 2019.

Crossed Swords (since 2016) focuses on developing tactical responsive cyber defence skills of cyber experts. The exercise aims to help practice the skills required to fulfil the role of the Red Team and offer the most cutting-edge and challenging training experience for national cyber defenders. In 2018, for the first time, the exercise brought together critical information infrastructure providers, military units, and specialised military equipment.

In addition, the Centre is regularly contributing to the wide array of cyber defence exercises, including the NATO's largest cyber defence exercise – Cyber Coalition – and other technical and strategic level training events.

▶ **CYCON INTERNATIONAL CONFERENCE.** The Centre is known for its forward-looking mindset and as such, is an acknowledged facilitator of strategic discussions – both publicly at the CyCon conference and behind closed doors in NATO's corridors. CyCon, the annual International Conference on Cyber Conflict, addresses the most relevant issues concerning the cyber defence community. In the ten years of its existence, CyCon has become a community-building event for cyber security professionals, adhering to the highest standards of academic research and bringing to



Flag-raising ceremony to mark the accession of Bulgaria, Denmark, Norway and Romania.

Tallinn somewhere around 600 decision-makers, opinion-leaders, top military brass, as well as law and technology experts from the governments, military, academia, and industry of about 50 countries.

► **TALLINN MANUAL AND OTHER RESOURCES.** The Tallinn Manual 2.0 is the most comprehensive interpretation of existing international law in the cyber context, offering insight for policy advisors and legal experts on how international law applies to cyber operations carried out between and against states and state actors. An invaluable analysis by an international group of renowned scholars, published in 2017, it serves to inspire both academic research and state practice.

The Cyber Commanders' Handbook, to be published in 2020, will provide guidance for Cyber Commanders, their staff and subordinate entities to support the planning, coordination, execution and assessment of cyber operations. The Handbook presents the overall contexts in which a cyber commander needs to operate and introduces the roles, responsibilities and core activities of a Cyber Command. It does not address the "how" of those cyber operations but rather focuses on the "what" and "why" of those duties.

The Handbook is a product of a coordinated team effort by the CCDCOE and experts from national cyber defence entities. It is a first multinational effort to characterise, from the perspective of a Commander, the planning, coordination, execution and assessment of cyber operations.

The Centre is also hosts the Interactive Cyber Law Toolkit, an online resource for lawyers and practitioners that was launched at CyCon 2019. The practical Toolkit consists of several hypothetical scenarios, each of which contains a description of cyber incidents inspired by real-world examples and accompanied by detailed legal analysis; for example election interference, power grid disturbance, economic espionage,

and armed conflict, to name a few. The project is run by a consortium of five partner institutions: Czech National Cyber and Information Security Agency (NCISA), International Committee of the Red Cross (ICRC), NATO CCDCOE, University of Exeter, and Wuhan University.

The Centre's publications and research papers are available online in the Cyber Defence Publications Library on the Centre's website. The CCDCOE's law research extends well beyond the Tallinn Manual.

► **ANALYSIS AND TRAINING.** The pursuit for technological innovation is accompanied by concerns about cyber security, with implications to a broader national security context. A recent research paper published by the CCDCOE takes a look at the cyber security debate around Huawei as the potential supplier of 5G technology for the next generation of wireless networks. Given the growing dependence of modern societies on digital infrastructure and communications technology, many countries are growing uneasy about introducing a critical reliance on equipment that can potentially be controlled by non-democratic states in peacetime and in crisis. The paper argues that 5G rollout needs to be recognised as a strategic, rather than merely a technological choice. Considering the strategic and legal issues raised regarding the potential reliance on Chinese technology in the rollout of 5G, the paper explores the national responses, and offers recommendations for a common approach.

CCDCOE promotes life-long learning in the field of cyber security. The training courses arranged by CCDCOE are based on the latest research and cyber defence exercises of the Centre. CCDCOE is committed to continually improving the training offerings to address the changing needs of the ever-developing cyber security field. To best meet the training requirements of our allies, partners, and NATO as a whole, courses are provided in different formats and locations, covering a broad range of topics in the technical, legal, strategic, and operational cyber security domains.

In 2018, the Centre was assigned by the NATO Allied Command of Transformation the responsibility to coordinate NATO's education and training in the cyber field. As such, the CCDCOE translates NATO's training requirements for cyberspace operations into education and training solutions and coordinates all the efforts to overcome the identified gaps in individual and collective training issues. ■



Participants of the red-teaming cyber capabilities exercise Crossed Swords.



REPUBLIC OF ESTONIA
MINISTRY OF DEFENCE

Defending the Nation Needs Steady Planning

The Ministry of Defence is responsible for organising national defence – for deterring attacks against Estonia and ensuring that Estonia is capable of defending itself against external threats. Ministry of Defence organises and ensures national cyber defence in cooperation with the Estonian Foreign Intelligence Service, Estonian Defence Forces Cyber Command, and Cyber Defence Unit under the Estonian Defence League.

▶ The Estonian cyberspace is part of the safe and stable global cyberspace. Whereas cyber security is founded on constant and close international cooperation, cooperating and communicating with allies and partners is essential. Contributing to the work of international organisations – primarily the European Union and NATO – and participating in bilateral, regional, and global cyber security related formats is integral part of international relations. Analysing the international law that supports cyber security and applying it in the Estonian legal system, as well as developing cyber standards has an important role.

In 2019, Estonia and the United States started a cooperation to build a joint platform for sharing cyber threat intelligence between the two countries. The cooperation is based on a joint R&D cooperation agreement between the United States Department of Defence and the Estonian Ministry of Defence, signed in 2016, whereas the collaboration was initiated already in 2014 in cooperation with the US Air Force Research Laboratory (USAFRL) with the idea of automating data exchange for cyber threats.

The Estonian Ministry of Defence established the Cyber Security Exercises and Training Centre CR14 in 2019. The Centre operates under the Ministry of Defence and serves the needs of the Estonian Defence Forces and NATO's Cyber Range as well as those of allies and partners.



NATO CCDCOE exercise *Locked Shields* uses the Estonian Cyber Range infrastructure.

The Centre will enable continuous international cyber defence training and developing cooperation between private companies in the field of cyber defence as well as with the academic institutions.

▶ In the near future, cyber defence training equipment belonging to the Defence Forces will also be installed on the Centre's premises. The Cyber Range is a system capable of imitating the functioning of a complex computer network and providing the opportunity to practice various cyber operations without endangering regular computer networks.

The Estonian cyberspace can be defended if the state and society as a whole participate in the defence, the necessary experts have been trained, and the society is aware of the dangers of the virtual world, knowing how to avoid them and acting correctly if problems occur. ■



REPUBLIC OF ESTONIA
DEFENCE FORCES

The Estonian Defence Forces Cyber Command – What Is It and What Does It Do?

The main tasks of the Estonian Defence Forces Cyber Command are to organise operations in cyberspace, managing the information and communication technology in the area of responsibility of the Ministry of Defence, ensuring cyber security in the domain, providing Headquarters support for the Joint Headquarters, preparing and forming wartime and reserve units, leading and coordinating the development of cyber and management support capabilities, supporting the strategic communication of the Defence Forces and organising information operations.

▶ The Estonian Defence Forces Cyber Command was established August 1, 2018, joining together the cyber competence of the defence domain. The Cyber Command was formed on the basis of the Headquarters Support and Signal Battalion and the Joint Headquarters information and communication systems section.

According to Colonel Andres Hairk, Commander of the Cyber Command, the immediate goal of the Cyber Command is to achieve full operational capability to ensure the provision of services and information flow in the defence domain in an effective and timely manner. Like with any other information and communication technology and cyber agencies, one of the main challenges is recruiting new people. Today, the Cyber Command has vigorously recruited new people both from the labour market as well as from among the conscripts who have expressed a wish to remain in service.

In the coming years, the Commander of the Cyber Command wishes to further improve cooperation with allies and enhance national cyberspace

situational awareness in the defence domain. To achieve this, we plan to engage more conscripts in performing the tasks of the Cyber Command in cyberspace.

Cyber conscription allows young people with good technical skills to continue their professional development and contribute to national defence with their skills and competence. In the beginning of the cyber conscription service, the conscripts will receive basic military training, after which they will undergo professional training and will perform practice in the provision of services or capability development.

During its nearly one and a half years of operation, the Cyber Command has made significant progress in improving national cooperation and has contributed to the development of comprehensive national defence. In 2019, the Cyber Command entered into a cooperation agreement with the Information System Authority (RIA) to practice both inter-agency cooperation and cooperation with other civilian structures in various exercises and to enhance information sharing between the institutions.

Much attention has also been paid to educating users through a cyber-hygiene course, which has raised the users' awareness of cyber related security risks and therefore contributed to raising the level of cyber security in the defence domain.

► In addition, in 2016, a defence research and development agreement was signed between the ministries of defence of US and Estonia, under which a cooperation project has been launched to develop an automated cyber threat intelligence exchange system between the US Air Force and the Estonian Defence Forces as well as the development of a software system for a more comprehensive threat intelligence exchange between the defence forces of the two countries.

Every year, the Cyber Command also participates in various international exercises, such as the Cyber Coalition and the Spring Storm, which focus on practicing both national procedures and cooperation with allied forces. For years, the Cyber Range of the Cyber Command has provided a virtual cyber range environment for conducting various NATO and allied forces exercises, enabling allies to practice, validate, and test concepts, technologies, and people. The most well-known training exercise supported by the Cyber Command is Locked Shields, organised by the NATO CCD COE, the largest live-fire technical exercise involving more than 1,200 experts from 30 countries. ■





Cyber Defence Unit

Cyber Defence Unit: Preparing For The Storm

The Cyber Defence Unit (CDU) of the Estonian Defence League (EDL), based on a volunteer initiative, is a national collaboration model for cyber security professionals and technology experts, structurally integrated into Estonia's voluntary National Defence organisation, the EDL. CDU's main role is to develop and provide cyber reserve for providers of vital services, government agencies, and the Estonian Defence Forces (EDF) in times of crisis.

► Founded after the broadly reported 2007 cyber attacks in Estonia, the first official cyber defence units were de facto formed in 2009 within the Estonian Defence League's existing territorial units of Tartu and Tallinn. On 28 January 2011, the CDU was formally established as an extraterritorial branch within the EDL. Informally, the CDU is still also known as the (Estonian) Cyber Defence League (or 'Küberkaitseliit' in Estonian).

A milestone in the development of the unit was reached in December 2018 with the opening of the first-ever own premises, located in the southern outskirts of Tallinn, together with the Harju district of the EDL. Today, the CDU also has representation in Tartu (the second largest and a historical university city) and two new regional subunits in Pärnu and Jõhvi.

The Estonian Defence League Act (EDLA) explicitly integrates the CDU into the national defence system, providing it with a legally established objective and a framework for structure, management, membership, and functioning. The law also foresees engaging the EDL in ensuring cyber security under the leadership of a competent authority. This means the CDU is not operating independently as a 'lone ranger', but always based on the direction of a relevant agency (for example, the Information System Authority or the EDF Cyber Command). However, when providing supportive or preventive activities for cyber security, such as awareness raising, there is more freedom and space for creativity.

One of the strengths of the Cyber Defence League is diversity: our members come from very different walks of life, each with their own background and civil or military skillset. Members of the CDU are volunteers, not contracted experts. They basically contribute for free, without monetary remuneration. Only some expenses for transportation, accommodation, and food are compensated when on duty or participating in training events.

All members must go through a vetting procedure to obtain a security clearance relevant to their position within the CDU structure. The CDU is focused on strengthening the professional cyber defence skills of its volunteer members in order to prepare and enhance support capabilities that can be provided in a cyber emergency, where our members act as force multipliers.

▶ In addition to domestic activities and exercises, CDU has always engaged with international partners, the Maryland Air National Guard (MDANG) in particular. The relationship dates back to the early days of the CDU. Also, the EDL and Estonia have been Maryland's State Partner for more than 25 years. In 2020, there is a larger bilateral CDU/MDANG Ex Cyber Ghost in the planning. In October 2019, the CDU team prevailed and won an international paintball competition (taking place in the imaginary cyber city Alphaville, MI), organised by the Michigan NG. As one of CDU's founding members, Lt Gen (Ret) Johannes Kert, Estonian CHOD 20 years ago and currently serving as MP, has put it: 'In cyber, size does not always matter. This is the reason why a small country can also engage with the US cyber counterparts as equal partners.'

Apart from the US, our other priority international engagements have been: Latvia, due to having a similar model for cyber reserve and physical proximity; Ukraine, as this is where the real and recent experience with the potential opponent's modus operandi comes from; and previously also Georgia, for similar reasons. We have felt a certain moral obligation to share best practices, help other countries in distress, particularly those we have historic ties to and personal relationships with.

There have been a handful of cases in the past five years when CDU's involvement has been officially requested according to the above procedures. These have ranged from organising high-level exercise scenarios and PEN-testing to open source monitoring and analysis during the Estonian presidency of the Council of EU and the Estonian ID-card vulnerability situation in 2017.

▶ March 2020 saw a different kind of a quiet storm arrive in the form of Covid-19, rather than a virtual virus. Nevertheless, the CDU was also called up with cyberspace monitoring and data analysis assignments. In addition, without formal request, our members have privately arranged collections and set-up of additional laptops for family physicians and drawn up alternative technical solutions for working remotely, outside their regular family health centres.

Next year, in January 2021, the EDL CDU celebrates its 10th anniversary. Now, with about half a dozen permanent staff members and membership of 'a few hundred', the CDU continues to develop, live up to its expectations, and make a difference. Indeed, size does not always matter. ■



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Engaging the Cyber Security Community At Home and Abroad

The Estonian Information System Authority (known by the Estonian acronym RIA) is home to CERT-EE, which monitors the Estonian computer network and solves cyber incidents, coordinates the safe implementation of IT infrastructures important for the state, conducts supervision, and raises awareness regarding cyber security. It is also a national contact point for international cooperation in the field of IT security.

▶ **WORKING WITH CRITICAL INFRASTRUCTURE PROTECTORS.**

Critical information infrastructure (CII) are those ICT systems that are essential for the proper functioning of our country. While each CII organisation is responsible for protecting its own systems and networks, we supervise and support that on the national level. We do this mainly through three work strands: assessing sectoral risks, giving guidance on how to reduce them, and raising awareness through training and exercises. As a good example of our hands-on support, we offered free penetration testing to seven companies in 2019, including two hospitals, two electricity companies and one water company.

Our main focus this year continues to be on the healthcare providers and the energy sector. The healthcare sector in Estonia is highly digitalised, which brings remarkable efficiencies, but also important risks that need to be mitigated. In 2017 – 2019 we have seen several incidents, including disruptive ransomware attacks against family clinics, which could have been avoided with proper cyber hygiene measures. Starting from 2022, family physicians will need to comply with stricter cyber security and data protection rules as they become subjects to the national Cyber

Security Act. To prepare them for this transition and improve their digital literacy in general, we are launching a series of trainings and workshops together with TalTech University and the Ministry of Economy and Communications which should reach up to 500 family physicians and nurses over the course of three years, starting from spring 2020. This will be in addition to the regular mentoring and trainings that we offer every year to different sectors to raise awareness on information security.

The energy sector continues to be important because all other vital services depend on it. In March 2019, we practised handling a ransomware attack against our main electricity transmission network company in a joint exercise for Estonia and Finland, with the national CERT teams working side by side with partners from the private sector. This year we will organise a live-fire exercise for the key cyber security personnel of five energy companies, so that they can practise solving a large-scale and complex cyber incident. We are also pushing for more cooperation among the energy companies of the three Baltic States, especially as all three nations are making efforts to achieve greater independence from the Unified Energy System of Russia / BRELL (Belorussia, Russia, Estonia, Latvia, Lithuania) energy ring. One way to share experience and mitigate common risks would be to establish a Baltic Information Sharing and Analysis Centre, which would bring together the entire energy sector of the Baltics. We have already tested this idea with our Latvian and Lithuanian colleagues and hope for some progress this year. Similar European and US organisations have proven their usefulness in raising cyber awareness in the sector.



► **BROADENING THE COMMUNITY.** An important lesson we have learned from past cyber incidents is that if a crisis occurs, we need to instantly bring in the best experts available in Estonia. We need a pool of people from the public and private sector that can work together as a team and find solutions through synergy. The highly-acclaimed international cyber exercise Locked Shields plays an important part in achieving that goal, but in addition, we are planning to launch a national live-fire exercise together with the Cyber Command and Defence League's Cyber Defence Unit. The exercise would involve IT staff from various public and private sector organisations and would also serve as a national trial before the Locked Shields. Most importantly, it would help broaden the community of experts that have regularly practiced together and could support the CII sector in case of major incidents.

CYBER SECURITY SERVICE OF RIA

One of the main tasks of the Cyber Security Branch of the Estonian Information System Authority (RIA) is to be there for the wider cyber security community in the country to offer both guidance and support. We do this in a number of ways.

- The Incident Response Department CERT-EE is always only a phone call, an e-mail, or a tweet away, while also producing a detailed cyber newsletter every morning. To reduce the time needed to detect and respond to cyber incidents in Estonia, they also offer different freely available technical solutions, the most important of which is Suricata-4-All (S4A), a free-ware-based network traffic analysis system that makes it possible to detect attacks and malware – and in some cases, vulnerabilities and configuration problems as well.
- The Analysis and Prevention Department compiles weekly, monthly, quarterly, and relevant ad hoc overviews or analyses of the Estonian cyberspace and has started to conduct major awareness-raising campaigns on cyber hygiene and security. The one coming this autumn will focus on small and medium-sized enterprises.
- The Critical Information Infrastructure Protection Department advises the relevant service providers and sectors on best practices and also provides penetration testing services. In addition, they organise a number of different exercises every year – some of which take place alongside other countries, but some are more focused on the key Estonian businesses.
- The Standards and Supervisory Department manages and develops the Estonian National Information Security Standard (ISKE) and advises and supervises its implementation. In 2020, work will continue on writing a new information security standard to make it easier to implement and more practical to use on a daily basis. Because of the rapid development of the IT sector, many organisations have become more mature and capable of applying a more risk-based approach and can assess their needs and possibilities for cyber security more precisely. Although the new standard has many structural innovations and substantive changes, the main principles of remain, e.g. just like a front door, a computer must be kept locked.



Cyber Capacity Building – Cyberspace Has No Borders

▶ For Estonia, the issue of investing into other countries' cyber capacity is essential. When drafting its 3rd national cyber security strategy in 2018, Estonia established the promotion of sustainable cyber security capacity building (CCB) across the globe as one of its national priorities. CCB is a broad issue and it can have different forms and topics, from educating one's peers to sharing specific expertise in faraway locations.

Sustainable capacity building depends on the credibility of the experts and their expertise in turn relies on practical experience. As 'cyberspace has no borders', it is essential that the various capacity building initiatives in the frameworks of international organisations as well as those undertaken bilaterally nevertheless allow for a unity of national effort.

As the host and the framework country for the NATO Cooperative Cyber Defence Centre of Excellence since 2008, Estonia has a strategic interest in promoting cyber security cooperation and mutual learning between like-minded countries. Estonia also plays an active role in NATO's other external partnerships, such as the cyber security part of the Substantial NATO-Georgia Package that aims to improve Georgia's defence capabilities, increase its resilience, enhance interoperability with NATO, and support its NATO membership process. In line with similar Euro-Atlantic ambitions in Ukraine, Estonian experts, in particular from the private sector, have conducted a number of cyber security capacity building events related to cyber hygiene, cyber security of elections, strategic decision-making in cyber crises, etc.

▶ An area of increasing importance for Estonia is CCB in the European Union framework. Since 2019, RIA is the host and lead of EU CyberNet — the EU's prime new CCB initiative. As the world's largest donor of development cooperation, the EU is increasing its assistance to third countries in the areas of digitization and cyber defence, as well as developing cooperation and professional skills among Member States' cyber experts. EU CyberNet will establish an EU-wide network of cyber security experts that can be used by the Member States and EU institutions to carry out cyber security assistance projects in third countries. The current target of the network is to include more than 500 experts and 150 partner institutions, ranging from national cyber security centres to universities and think tanks.

Another important capacity building project for RIA is the EU Cyber Resilience for Development Project, or Cyber4Dev. It aims to increase cyber security in Africa, Asia, Latin America, and the Caribbean through topical training programs. The project assists participants in developing and implementing cyber security strategies, enhances the capabilities of the CERTs, and supports regional and international cooperation. For instance, the project has supported the creation of a CERT in Botswana and the development of Sri Lanka's CERT Incident Management Capacity, helped the Rwandan Centre for Cyber Security to draft the first national cyber strategy,



Risk assessment training by Estonian experts in San Jose, Costa Rica.

advised Sri Lankan cyber security law makers and eID developers, trained CERTs for incidents in several African countries, and organised the first national cyber security exercise in Mauritius. In 2019 alone, the Cyber4Dev project hosted 48 events with a total of 28 experts and over 400 trainers.

► **WHERE TO NEXT?** Why is the success of the CCB important for the EU as well as Estonia? Because both Estonian and European cyber security literally begins from outside Europe. Many countries around the world are undergoing an ultra-fast digital transition, using innovative digital platforms, experimenting with financial and mobile technologies, using off-line renewable energy solutions, and supporting the emergence of domestic businesses. It is also a fact that in addition to EU's development cooperation efforts in the developing countries, many other parties, such as China, are investing heavily into infrastructures and technological solutions abroad, with some of their activities hinting at an outcome where their technology comes with a heavy dose of geopolitical pressure.

Against this background, questions on how secure is the national cyberspace, how up-to-date are the laws, how appropriate are the institutional roles and responsibilities, what is the national level of preparedness to identify cyber threats, and how effective are the tools to manage incidents will remain pertinent for years.

The challenges that capacity building deals with will only grow and could be particularly far-reaching in the 2020s, as the world moves from fourth-generation information networks to the fifth, introducing a significantly higher technological capacity. For Estonia, living up to this should thus be a good challenge to face — as capacity building could very well support the deliberations back home too. ■



Making I-voting Even More Secure And User-friendly

The Ministry of Economic Affairs and Communications (MKM) is the leading ministry in the area of cyber security. In addition to digital development and cyber security, it is also in charge of the policies of trade, energy, construction, transport, media services, and other areas.

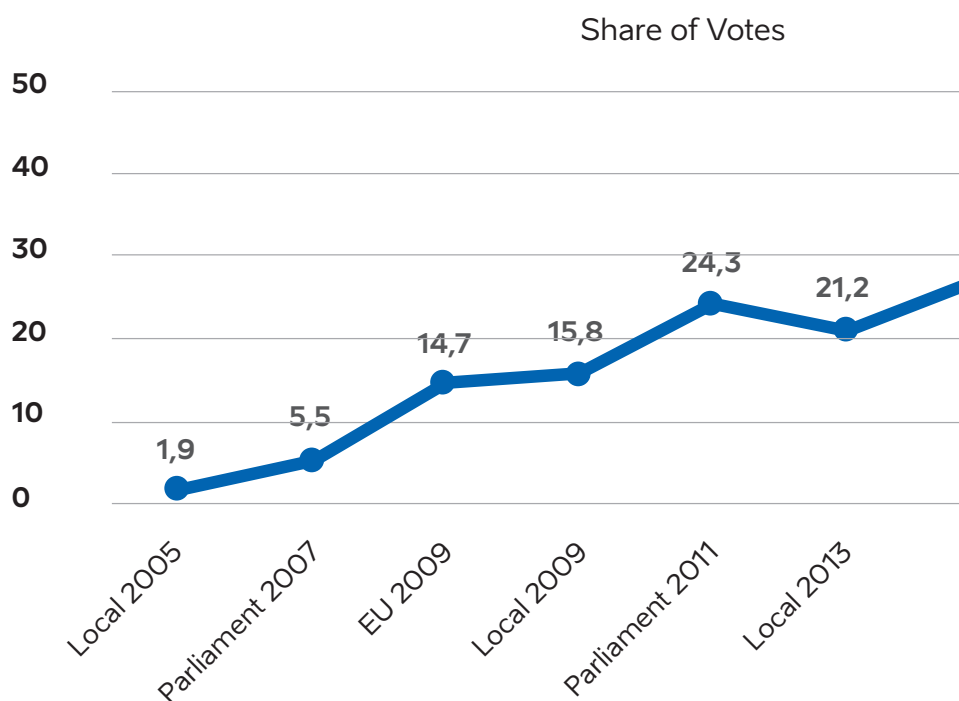
▶ Since 2005, Estonia has been the only country where it is possible for citizens to vote online, be it in municipal, national, or European-level elections. The aim of introducing such a possibility was mainly twofold:

1. making the election process simpler and more comfortable for both the voters and the organisers;
2. building on and developing the capacity of the Estonian government to enable citizens to interact with the state as electronically as possible (which also reinforces the first aim).

From then on, Internet voting or i-voting has been a secure and increasingly popular option for casting ballots. Unlike the electronic voting systems used in some countries, no special machinery is needed. Estonian i-voting can be done from anywhere in the world. The whole process from logging in to confirming your vote with an electronic signature takes only around three minutes on average.

The share of votes cast online has been steadily going up throughout the years. Back in 2005, when the system was introduced, only 1.9 per cent of voters did so electronically. During the 2019 election for the European Parliament the corresponding number was 46.8 per cent, which means almost half of the people who decided to take part did so from the comfort of their own home or office.

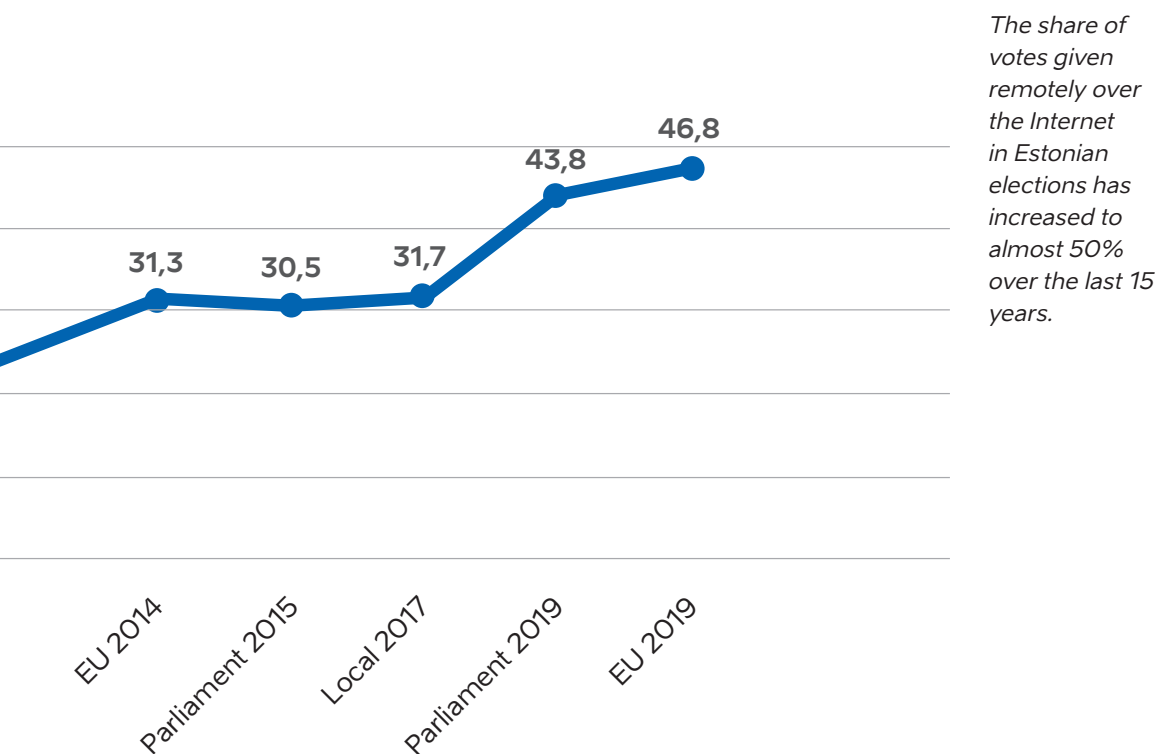
I-VOTING



▶ As the security of the system is treated as a key priority, and respective preparations by the Estonian Information Security Authority (RIA) and the State Electoral Office, the two state institutions responsible, have been more and more comprehensive year-on-year, no (real) security incidents or cyberattacks have been detected. The last time around, cyber hygiene courses for candidates and their campaign teams were also offered, as well as an opportunity for all political parties to check the security of their websites and e-mail servers.

The coalition government formed after the March 2019 parliamentary elections decided to put even more emphasis on the security of i-voting. This happened not the least because of the attempts in recent years to influence election results in countries such as the United States, France, Bulgaria, and the Czech Republic, but also to address different questions that had been raised by some members of the public over the years. In June 2019, a working party on the security of i-voting, consisting of government officials, information technology experts, members of academia, and outright critics of the system, was established by the Minister of Foreign Trade and Information Technology.

For six months, the working party looked at the issue with broad perspective, examining various different aspects, including the regulatory framework, financing issues, raising awareness, and technological



questions. The main findings of the working party were published just before Christmas in 2019:

- Sustainable financing is needed for the maintenance and development of the i-voting system;
- The system should be made more comprehensible for the general public;
- The choices made in developing the system should be better communicated;
- The number of people involved with the safety and the security of the system should be increased.

The results of the discussions of the working party will be taken into account in developing the i-voting system further. The State Electoral Office (responsible for the whole i-voting system) has to make the decisions in cooperation with the development and security partner, the Estonian Information System Authority. For example, thus far it has been possible to vote online only during the so-called advance elections (from the tenth to fourth days before election day), but that could change with the adoption of the next version of the elections information system. Another possible deliverable on the horizon could be the added option of voting via one's mobile phone. Many of these decisions, though, need legislative approval. ■



REPUBLIC OF ESTONIA
DATA PROTECTION INSPECTORATE

Protecting Personal Data Becomes an Issue of Trust

The Data Protection Inspectorate defends the constitutional rights to obtain information about the activities of public authorities, to the inviolability of private and family life in the use of personal data, and to access data gathered in regard to oneself.

► In a country of 1.3 million inhabitants, we registered 115 infractions of data protection regulations in 2019. Most of these incidents could be considered non-significant. But even non-significant events have the potential to benefit cyber criminals.

The Data Protection Regulation requires notifying the Estonian inspectorate whenever unauthorised persons have gained access to personal data. This could be access to a server, computer, or paper documents. If the processor of data were to discover illegal downloading, copying, or other processing of the personal data, it is an infraction which needs to be reported to the inspectorate within 72 hours.

The incidents recorded in 2019 can generally be divided into two categories. On the one hand there were incidents where the root cause could be identified as the software used. On the other hand — for the majority of the incidents last year — the root cause was human error. This could be an actual error, but also carelessness or negligence. In multiple instances, we were notified of mistakenly sending sensitive information to the wrong e-mail address. There were also reports of misconfiguration of databases, resulting in unauthorised access to this data.

There were other incidents which were caused by insufficient attention to details or lack of knowledge regarding data protection. Just



responding to phishing e-mails or entering your data there is an example. Even though all data processors should be able to use elementary security protocols and technologies to keep phishing e-mails from getting through to end users, basic DMARC protocols or STARTTLS encryption methods for secure e-mail exchange are still not widely in use.

▶ The largest potential data leak could have come from a local bike-sharing initiative at an Estonian municipality, had it not been for the prompt action taken by the owners of the service. The database behind the ride-sharing service had 20,000 names, contact information, user ID-s, use logs, and connections with other public transportation logs. Thanks to the quick reaction by the processor of the data following the discovery of this vulnerability, there was no real threat of personal information being leaked and after an investigation into the matter, the Data Protection Inspectorate issued only a written reprimand regarding the case.

There were some cases of infractions where the developers of a system did not pay enough attention to protecting personal data at an early phase of development. This led to some incidents at online self-service environments where customers unintentionally saw the personal details of another customer. These types of incidents could have been prevented by using privacy-by-design policies at early product design phases.

▶ How services handle data protection and how well they know the rules behind data protection is becoming a question of competence and trust. The larger the potential damage to trust or sales from data leaks, the faster the processors of the data fix their services and databases. ■



EISA: A Collaborative Effort to Boost Estonian Cyber Security Potential

The Estonian Information Security Association (EISA) was founded to boost cross-sectorial cooperation in Estonia between academia and the private sector as well as with the government. EISA intends to enhance R&D activities in the information security and cyber security field in Estonia.

▶ Estonia is visited by hundreds, if not thousands, of delegations each year who marvel at our digital ecosystem. It is often not the 'what' that amazes them, but the 'how' — and sometimes the 'why'. The 'how' has, for nearly three decades, stood upon the idea of unfettered collaboration between the private sector, academia, and the government. Stemming from an imminent need to find and execute solutions to urgent problems, the public-private partnership model has been in the DNA of e-Estonia since the very beginning. What once started as a close-knit community has now grown into a flourishing ecosystem, combining stakeholders across all sectors, garnering global attention.

History has also offered several good crises for Estonia to test the sustainability of its community, alongside the resilience of its cyber capabilities. From the attacks of 2007 to the more recent incidents, the crises have been overcome by the companies and universities stepping up and offering solutions to our digital infrastructure providers. History has provided us with opportunity and structure, but the focus on a unique community and competence is what distinguishes us from others.

There is potential for so much more.

In 2018, the Estonian Information Security Association was founded by BHC Laboratory, Clarified Security, Cybernetica, and Guardtime along



People all over the world visit Tallinn to marvel at Estonia's digital ecosystem.

with Tallinn University of Technology, with the aim of providing a unified platform for companies, organisations, and academia to partake in large-scale international projects, to enhance and facilitate information sharing, and to provide a common forum for discussions for experts across different fields. Ecosystems are built on thriving communities, and communities are built on common goals.

Centralising decreases resilience. This is true for all systems, and the idea of distribution is engrained in the Estonian mindset. EISA follows the same principles, facilitating between stakeholders, rather than creating a central cluster. Cyber security competence in Estonia is set where it creates more value, and distributed across the private sector, academia, and the government. The limited availability of workforce (a global challenge in the IT industry) ensures that each stakeholder holds its competence for the most critical function — and collaborates where necessary.

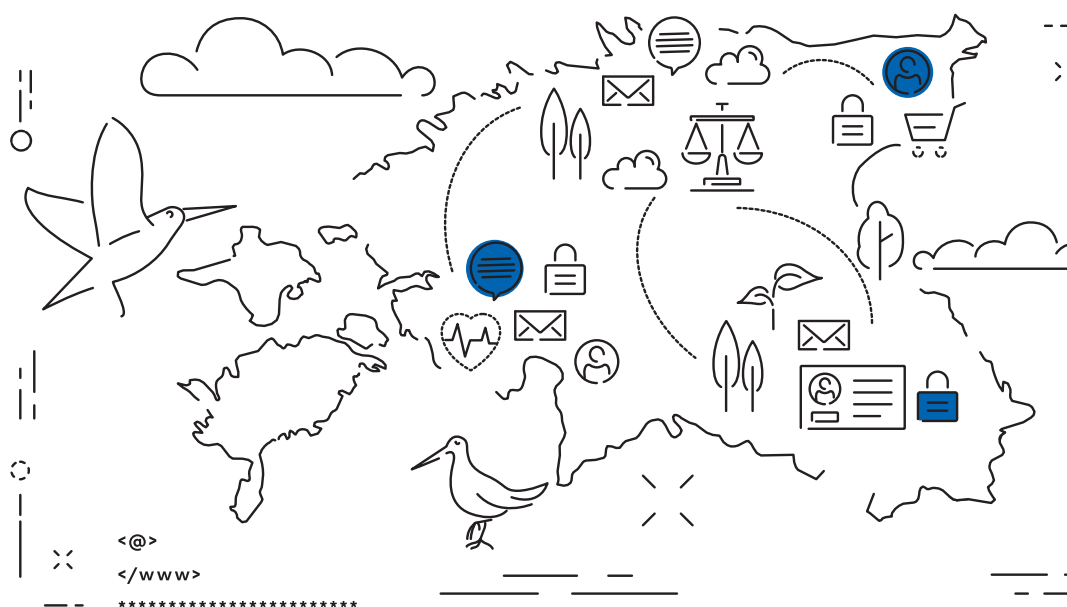


EISA has the ability to enhance the intrinsic disposition for collaboration and to become a central consolidator for the Estonian cyber stakeholders. Partnering closely with the government allows for exchanging expertise at a new level. EISA participates as a member

on the National Cyber Security Policy Council and is a member of the North European Cyber Security Cluster (NECC). While locally, our aim is to strengthen cross-sectorial cooperation, on the European level we can provide a wider impact and bring a united offering to the European cyber security ecosystem.

Harnessing that potential needs a strong shared vision, but relies heavily on the trust between all stakeholders. We have long-lasting examples of these partnerships — from building the X-Road with the Information System Authority to providing input for decision-makers here, and abroad, with our cryptographic algorithms lifecycle report, published since 2011. All the founding companies of EISA have stellar examples of cross-sectorial collaboration: BHC Laboratory launched a cyber hygiene module for the MBA program of the Estonian Business School and has trained the top civil servants on overcoming cyber crises in Estonia; Clarified Security cooperates with the NATO CCDCOE, providing red teaming services for the world's largest cyber defence exercise, Locked Shields; Guardtime provides its blockchain technology to protect the most critical logs in Estonia (e.g. health records). These are but a few of the examples of the successes already in place — but again, there is potential for so much more.

Once we take the leap from focusing on the 'what' and 'how' and starting defining and, more importantly, focusing on the 'why', we will be able to not only stand by but lead the processes that design the cyber arena of tomorrow. For tomorrow, not only are the established players important, but also the new ones, the entrepreneurs that can derive their experience and competences from the unique ecosystem we have here in Estonia. The map is not the territory. ■



Photos and illustrations:

Front cover, pages 14-15, 52: Bluecat Animation Studio

Back cover, pages 42, 49: Brand Estonia Toolbox

Pages 5, 7: Kristi Sits

Page 24: Anders G Warne

Page 27: Ministry of Foreign Affairs

Pages 31, 33, 35: NATO CCDCOE

Page 32: Estonian Defence Forces / Ardi Hallismaa

Page 37: Allan Vool

Page 41: Renee Altrov

Page 44: Liina Areng

Page 51: Magnus Heinmets

