# Trends and Challenges in Cyber Security

## 1. Russian aggression in Ukraine – is it also a cyber war?

### SITUATION
Russia’s military aggression against Ukraine has also manifested in cyber space in various ways. Since the beginning of the year, there have been many denial-of-service (DDoS) attacks against Ukrainian businesses, state agencies, and other organisations and defacements of websites where the attackers have replaced contents with their own messages.

The most extensive attack since the beginning of the invasion occurred on March 28 against Ukrtelekom, the largest telecom company of Ukraine, which left roughly 80% of the customers without the Internet for hours. Other attacks of a lower impact have also been conducted against the telecommunication sector and the direct military activity obviously also causes service interruptions.

The personnel of Ukrainian state agencies and armed forces, but also common Ukrainian citizens receive malware and phishing e-mails on a massive scale. International organisations operating in Ukraine have also been targeted, as well as European officials dealing with Ukrainian refugees and coordinating assistance.

Cyber attacks have also been used for spreading false information. For example, the websites of two local governments were compromised, posting messages about Kyiv having surrendered. A deepfake video of the Ukrainian president Volodymyr Zelensky was spread on compromised Ukrainian news portals (e.g. Ukraine 24).

Furthermore, at least five different types of data wiping malware have been launched in the direction of Ukrainian authorities and businesses since the beginning of the year, deleting data from infected devices and rendering them unfit for use.

### ASSESSMENT
The majority of the cyber attacks against Ukraine so far have been fairly primitive – such attacks fail to derail the country or surrender it to the attacker’s will. The case of Ukrtelekom was a more serious attack against critical infrastructure, but in general the cyber attacks so far have been less devastating than had been expected. There may be several explanations for this:

1) Cyber attacks are a tool for demonstrating one’s power in an unconventional manner by using a so-called ‘grey area’ which disappears when physical war has begun;
2) More destructive cyber attacks may spread to other countries and Russia is wary of this, trying to avoid further escalation with the West (for now);
3) Russia will start applying its cyber capabilities against Ukraine and the Western countries in a later stage when the military activity has stalled and the effects of the sanctions are felt more deeply.

Cyber attacks against the West might also not result in any geopolitical gains for Russia in the current phase. Instead they might bring even more unity between the West and Ukraine. However, Russia is actively operating within the so-called ‘grey area’, using cyber attacks as part of information operations and for interrupting services, in addition to intelligence gathering.

The cyber vandalism and crime in Russia will also continue to proliferate freely, as long as their targets match those of the Government. Thus, the level of the cyber threat is currently relatively high for Estonia and other Western countries, as those countries which have vocally supported Ukraine, sent assistance, and imposed strict sanctions on Russia may become a target for revenge.

## 2. Estonia is increasing its resilience in the cyber space

### SITUATION
The direct impact of the war in Ukraine on the Estonian cyber space has been limited so far, the number of significant incidents remains at the normal level and no life-disturbing attacks which could be linked to the conflict have occurred. CERT-EE has, however, observed the following:

1) Vulnerability scanning from foreign IP addresses was more active than usual in February and March. This concerns particularly the public sector and the financial sector.

2) Attempts to spread malware over e-mail are made on a massive scale (mostly different versions of the Trojan malware which are contained in a document attached to an e-mail message and activated when the document is opened). We have seen such waves before but the current volumes are higher than normal. In some cases, war-related topics are used as bait, but previously used topics are more common (invoice, price offer, etc.).

3) There have been a few, rare incidents which may be politically motivated. For example, a community newsletter was hacked to remove information about the Ukrainian conflict. Some denial-of-service attacks against media companies have also occurred.

4) A few cases of random fraudsters attempting to use themes related to Ukraine to defraud people of their money are known as well.

### ASSESSMENT
The geopolitical tensions and conflict will probably last for a long time and even if the war in the kinetic world eases and subsidiaries at some point, this may mean an expansion of the conflict in cyber space. The threat of cyber attacks in the form of specific targeted revenge action (DDoS attacks, defacing, data theft and/or disclosure) or supply chain attacks with extensive spillover (compromising a large service provider or a widely used software component) is considerably higher than usual.

What to think of the aforementioned vulnerability scanning? In principle, it is a common activity in the cyber space, used by regular cyber criminals, organised groups, as well as state-sponsored actors who scan their potential targets in this manner. The purpose of the scanning varies depending on the client, including, for example, stress testing of a website, identifying software with exploitable security vulnerabilities, or simply scraping contacts from websites to send them phishing or malware files. The scanning does not mean that all weaknesses will be exploited, but the presence and failure to patch them increases the likelihood of attacks. In the current security situation, each individual, agency, and business must do everything they can to reduce their vulnerability to attacks.

The Information System Authority (RIA) – like the cyber authorities of several other countries – has issued threat assessments and advice (in Estonian) on how to protect oneself in the cyber space. The national state network managed by the Information System Authority which covers the majority of the public sector has been strengthened with an additional firewall since February which identifies and stops thousands of attack attempts every day. Several vital service providers have also strengthened their defence measures and are regularly consulting with the Information System Authority on the latest threat landscape. So far, the aggressor has used its potential in the cyber domain modestly, but we must be prepared in case that changes.
3. A new wave of hacktivism

**SITUATION**

Not only countries, but also several malicious cyber groups and ideologically motivated hackers, also referred to as hacktivists, have chosen sides in the ongoing war.

The international hacker group Anonymous has claimed responsibility for several attacks against Russian state agencies and other organisations, and organised several attacks against Russian national television channels, replacing content with videos of the Russian destruction in Ukraine.

The Ukrainian government has called up all volunteers with IT skills to join the so-called 'IT army' which carries out denial-of-service attacks, defacing, as well as more complex operations against Russian websites and businesses. The hackers and groups supporting Putin are also not sitting around – for example, ransomware group Conti and the hacker group Killnet have expressed their support of the Kremlin. Even though there is a lack of certain evidence, Russian-supporting hacktivists are believed to be behind several attacks against Ukraine and attacks to spread false information.

**ASSESSMENT**

RIA strongly discourages Estonian people from going along with any calls to take part in cyber attacks, no matter how noble the causes.

Allowing an application in one’s phone to send false inquiries against some Russian propaganda websites may seem like a good opportunity “to do something”, but this is actually a dangerous activity. In principle, the user hands over their device to a botnet and runs an unknown code – obviously neither of those activities are ok from a cyber security perspective.

Such popularisation of DDoS attacks and a wide distribution of the technical tools (scripts) have already inspired others as well and there is information about some widely used websites in Ukraine which have been compromised, with the visitors’ devices receiving a command to start DDOSing certain websites. This happens without the user’s knowledge nor any control over the targets.

We will certainly be hearing a lot more about the activities of Russian- and Ukrainian-minded hackers and groups. We advise approaching such news with caution, as in many cases there is no independent confirmation or proof of who was behind the attack and whether or not the attack had the effect claimed by the group. Some claims of successful attacks may be part of an information operation or based on some other self-serving motives of the group.

Although the cyber area has been acknowledged as one of the domains of warfare for years, the rules applicable there still remain quite vague and it is often difficult to identify who should be held responsible for a certain attack. International hacker communities are making this picture even more confusing and adequate protection of citizens and services in the cyber space is becoming an increasingly difficult challenge for governments.

4. The CEO fraud scheme is back, but without much success

**SITUATION**

'Good morning! What is our account balance, can we make a €25,000 payment today?'

'Hello! I have an invoice which must be paid immediately, can you take care of it right now? Let me know so I can send you the bank details.'

These are extracts from fraudulent e-mails received by accountants, financial managers, or other employees of Estonian businesses or authorities in recent months. The sender of the e-mail appears to be the head of the same company or authority.

If such requests receive a positive answer, an invoice or the bank details are sent next. The fraudsters always stress that the payment is very urgent.

Reports of such CEO fraud schemes became more frequent in the end of last year and continued in January. CERT-EE received 44 reports of CEO fraud schemes in the first quarter, compared to 11 in the same period last year. The figure has multiplied four times.

The majority of those attempts fail: the recipient is aware of such schemes, he/ she becomes suspicious about the content or sender of the e-mail, or the company or authority has established strict rules for handling incoming invoices to reduce the risk of fraud.

Unfortunately there are also exceptions. In December, the accountant of an Estonian company transferred almost 15,000 euros on the fraudsters’ account. The same was done by an employee of another company in January with the damage amounting to the same level. In the latter case, the company had established the rules to avoid falling victim to such fraud, but the accountant ignored them considering the request to be very urgent.

**ASSESSMENT**

Although the rapid increase in the number of fraud attempts is concerning, the majority of the attempts fail and there are relatively few victims who have suffered financial damage.

However, we repeat the following advice:

- If you receive an e-mail from the CEO or CFO requesting urgent payment of an invoice, check the address of the sender. Hard-working fraudsters sometime falsify the e-mail address as well, but usually they only bother to change the name.
- Call the individual whom the e-mail is (or appears to be) from and ask if they have actually sent it. Use the number you know, not the one specified in the e-mail.
- If you suspect CEO fraud, forward the e-mail to cert@cert.ee.
- If you have transferred the money and then become suspicious, call your bank immediately to cancel the payment.
- Find out the proper procedure for handling incoming invoices in your organisation, and follow it without exceptions.

**GOING WELL::**

We see an increased interest of several sectors in cyber security since the start of the Russian invasion in Ukraine.

The Information System Authority meets regularly with stakeholders from the telecom, finance, and trade sectors to advise them on the current threat landscape and what to pay attention to. This also gives us a better picture on the cyber resilience of different sectors and what we can do to support them.

Threat assessments and current advice in Estonian can be found here (in Estonian) and warnings about ongoing campaigns on CERT-EE Twitter.

**COULD BE IMPROVED:**

The number of reports of user accounts having been taken over was above the average in the first quarter.

In most cases, this involved compromising social media or e-mail accounts and the attack affected several accounts together. For example, an individual’s Google account was accessed first and used to change the passwords of other related accounts. We advise using multifactor authentication and unique strong passwords in each environment to prevent this. It is also important to update your passwords regularly.