Republic of Estonia
Information System Authority



CYBER SECURITY IN ESTONIA 2025



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY



Cyber Security in Estonia 2025

Contents

FOREWORD

6 **Estonia's cybersecurity starts with you**
How can we tackle the record number of cyberattacks and security vulnerabilities we faced last year? **Gert Auväärt**, Deputy Director-General for Cybersecurity at RIA, explains.

OVERVIEW OF 2024

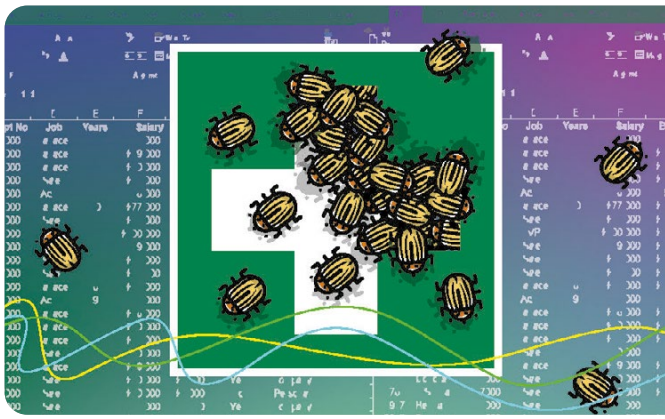
8 **Another record year we did not need**
No one expected 2024 to be a quiet year in cyberspace, but we also did not anticipate that the number of incidents with an impact would double from an already record-breaking level.

14 **Ukraine war: cyberattacks move closer to the frontline**
On 19 November last year, 1,000 days passed since Russia's full-scale invasion of Ukraine began. The battle in cyberspace has lasted even longer.

16 **SSSCIP chief: Russia operates more covertly in cyberspace**
We learn about the cyberattacks thwarted in 2024 through an interview with Brigadier General **Oleksandr Potii**, head of Ukraine's State Service of Special Communications and Information Protection (SSSCIP).



Photo: SSSCIP



18 **Lessons from a massive data leak**
At the beginning of 2024, criminals breached the server of Allium UPI, stealing the data of hundreds of thousands of Estonians.

20 **Russian intelligence ramps up cyber pressure on Western countries**
Cyberattacks against Estonian state authorities in 2020 were attributed to Unit 29155 of Russia's military intelligence (GRU).

24 **Phishers caught on the hook**
An international police operation shut down LabHost, a platform that provided services to phishing scammers, and the Estonian police played a key role in preparing the raid.

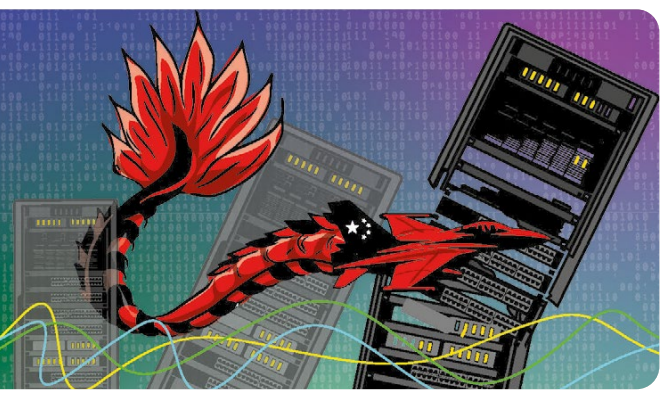
26 **DDoS attacks: more noise, less impact**
We registered an unprecedented number of distributed denial-of-service attacks (DDoS), but effective defence measures reduced the proportion of attacks with an impact.

28 **Fraudsters made off with millions**
Adding up the damage, we have to acknowledge once again that last year was highly profitable for scammers.

32 **Ransomware victims: schools and businesses**
Several companies, schools and even a dental clinic found their systems breached and data locked by attackers.

34 **2024 brought a record number of vulnerabilities**
Much to the advantage of attackers, users of vulnerable software were often slow to update it.

36 **2024: Events in the international cyberspace**
Last year saw influence operations surrounding elections, Chinese hackers breaching telecom companies, and a widespread IT system disruption caused by CrowdStrike.



40 **The Red Dragon spreads its wings**
China's ambition to become the world's leading power by 2050 is bolstered by its state-sponsored cyber groups.

SAFER CYBERSPACE

42 **Cybersecurity is a matter of national sustainability**
Cybersecurity is more than an IT concern – it is a matter of national sustainability, argue **Taavi Viilukas, Irina Klementi** and **Kaido Tee** from the National Cybersecurity Department of the Ministry of Justice and Digital Affairs.



44 **Estonian schools should prioritise cybersecurity**
The level of cybersecurity measures in schools varies widely, and the overall situation leaves much to be desired.

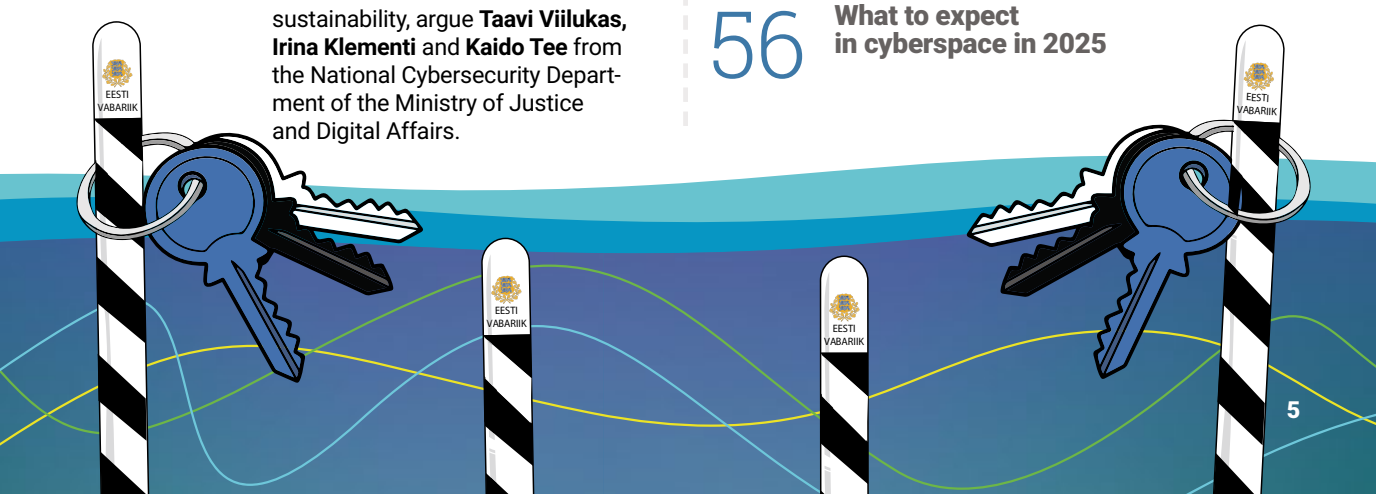
48 **Prevention efforts for all generations**
We conducted workshops for older adults, launched a campaign aimed at younger generations, and published guides for children and their parents.

50 **EU steps in cybersecurity**
What did the European Union achieve in cybersecurity in 2024, and what lies ahead in 2025?

52 **How can Estonia shorten its cyber borders?**
Over the past decade, the number of state-maintained databases has nearly tripled, significantly extending Estonia's cyber border, which requires monitoring and protection.

54 **I-voting: 20 years of progress**
The local government elections in October 2025 will mark the 20th anniversary of i-voting in Estonia.

56 **What to expect in cyberspace in 2025**



ESTONIA'S CYBERSECURITY starts with you

How can we tackle the record number of cyberattacks and security vulnerabilities Estonia faced last year? The answer starts with individual responsibility – strengthening your own defences first, then helping those around you, writes **Gert Auväärt**, Director of NCSC-EE and Deputy Director-General of RIA.

Let's begin on a positive note. Last year brought significant technological advances that opened new opportunities in both the economy and in research. However, this progress relies on increasingly complex digital infrastructure, which also creates more opportunities for cybercriminals.

A decade ago, few could have predicted the scale that cybercrime would reach. Today, it ranks as the world's third-largest 'economy', behind only the United States and China.

We have reached a point where cybersecurity must be seen as a basic necessity for individuals, businesses and states alike. Just as you make sure your wallet and keys are secure before leaving home, the same level of caution should apply when using a smartphone or computer to protect your data and assets.

DEFENDING ESTONIA'S DIGITAL BORDERS

RIA develops and manages the core foundations of Estonia's digital state while also acting as the backbone of national cybersecurity. RIA responds to threats, prevents incidents and safeguards Estonia's digital borders. To ensure the resilience of Estonia's digital society, cybersecurity must be strategically embedded across all sectors and adapted to local needs within international cooperation efforts. Alongside protecting state services, RIA also bolsters critical infrastructure and raises public awareness of cyber threats.

The new Estonian Cybersecurity Strategy 2024–2030 is focused on achieving these objectives. In light of the changing security landscape, we must review cybersecurity, information security and crisis management laws to uphold best practices and guarantee the uninterrupted operation of Estonia's services.

A RECORD YEAR FOR CYBERATTACKS

In 2024, RIA registered a record 6,515 cyber incidents with an impact in Estonia. Globally, a record-breaking 40,287 security vulnerabilities were identified – each a potential entry point for cyberattacks. These are not just numbers; they are a warning that cybercriminals have more opportunities than ever, the attack surface is expanding, and the overall threat landscape is deteriorating.



Photo: Jake Farra

Gert Auväärt

Hackers infiltrated US telecommunications companies, Romanian authorities annulled the first round of their presidential election due to cyber interference, and major data breaches and software failures shook the global economy. Cyberattacks are no longer just a technological issue: they affect elections, economies and even the fundamental structures of society.

Estonia's success as a digital state brings with it a significant responsibility. The number of national databases has tripled over the past decade, increasing the attack surface and highlighting the need for effective shared cybersecurity solutions – both in the public and the private sector. This is where RIA plays a crucial role: by providing central services such as X-Road and authentication solutions, we reduce redundancy and allow organisations to focus on their core activities.

Another key asset is RIA's unique cyber reserve, which is composed of experts from RIA, other state IT agencies and the Estonian Defence League's Cyber Unit. If a cyber incident severely disrupts a critical service and the affected organisation lacks the capacity to resolve it swiftly, RIA's cyber reserve can be deployed. This is not just a theoretical concept – it has already been activated on three occasions and tested in large-scale exercises at all operational levels.

EVERYONE HAS A ROLE IN CYBERSECURITY

At its core, cybersecurity is about people. The protection of personal and business data hinges on strong cybersecurity knowledge. That is why we placed significant emphasis last year on increasing cyber awareness. We organised well-received workshops for older adults, provided targeted guides for young people, and updated the prevention portal itvaatlik.ee with practical advice on recognising scams and reporting incidents. Not everyone needs to be an expert, but reliable information must be easily available. RIA's Cyber Test has already helped over 21,000 people improve their cybersecurity skills in just two years, making it a valuable tool not only for individuals but also for businesses and institutions.

> The protection of personal and business data hinges on strong cybersecurity knowledge.

As technology advances and cybercriminals refine their methods, we will likely face even more sophisticated threats in the future, including AI-driven attacks and large-scale data breaches. Sustainable security requires integrating cybersecurity into all processes and embedding it in everyday life.

This year's report is more than just a retrospective. It is a call to action – for individuals, organisations and the nation as a whole. Only by working together can we keep Estonia's cyberspace secure today and prepared for the challenges of tomorrow.

ANOTHER RECORD YEAR we did not need

No one expected 2024 to be a quiet year in cyberspace, as peaceful as a Sunday morning in a small Estonian town. But we also did not anticipate that the number of impactful incidents recorded by CERT-EE would double from the previous record high.

Last year, the number of incidents with impact soared to 6,515 from 3,314 the year before. CERT-EE's monitoring team, on duty around the clock, registered an average of 18 incidents per day. Where did this surge come from?

A SURGE IN PHISHING AND SCAM WEBSITES

Fortunately, the increase was not driven by incidents that shook the foundations of society or affected hundreds of thousands of people at once.

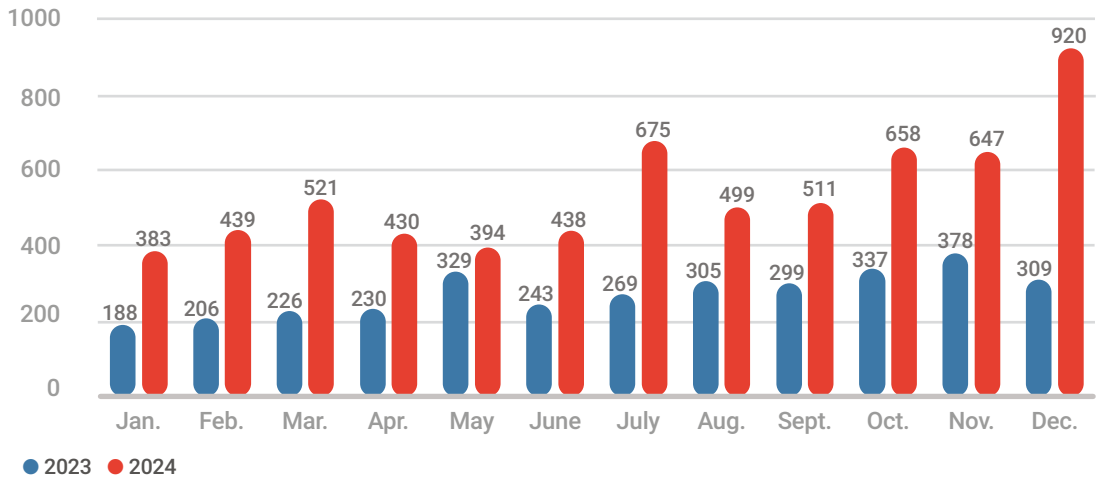
As in previous years, phishing and scam websites made up the majority of impactful incidents. Their number grew 2.5 times within a year, rising from half to two-thirds of all recorded incidents.

Phishing and fraud schemes come in many forms, like a patchwork quilt. Some scams are as classic as ever, such as fake banking websites that are nearly indistinguishable from legitimate ones. Victims think they are entering their PIN to access their account, but in reality, they are handing it over to fraudsters, who simultaneously access the actual banking website and empty the victims' accounts. Once the funds are drained, scammers often attempt to take out loans in the victim's name and transfer the money to their own accounts.

Fake delivery notices, sent in the name of well-known courier companies, also remain


PIN-kood
Mobiil-ID
ID-kaart
PIN-kalkula
Sisenen
Kiipkaart
Palun sisestage isikutuvastuse PIN (PIN1)
OK

Number of incidents with an impact by month



widespread. These messages direct recipients to fraudulent websites, tricking them into entering their bank card details under the guise of paying a delivery fee. Some victims fall for this even when they haven't ordered a package recently, only realising their mistake later when checking their bank statements and seeing not just a few euros withdrawn but hundreds or even thousands.

But when they finally try to withdraw their funds, endless excuses begin: delays, additional fees and new requirements.

Investment scams also spread last year, promising fantastic returns. After a temporary lull, alongside stocks, various cryptocurrencies – some more exotic than others – became a hot commodity for scammers once again. These frauds usually start small: victims 'invest' a modest sum, often just a few dozen or a couple of hundred euros. Their balance appears to grow over the next few weeks, and when they successfully withdraw their initial amount plus a supposed profit, their confidence (and appetite) grows while their scepticism fades. In the next round, they invest more.

As their displayed balance balloons, some, having spent their savings, even take out loans to maximise returns. But when they finally try to withdraw their funds, endless excuses begin: delays, additional fees and new requirements. In some cases, scammers demand further deposits to 'unlock' the money – deposits that, of course, are never returned. Eventually, the fraudulent website disappears altogether, leaving victims with nothing.

When CERT-EE identifies such scam sites, it requests their hosting providers to take them down, limiting the number of potential victims. However, our reach is not infinite. Ultimately, public awareness and critical thinking are the most effective defences against these schemes. Read more about various types of scams on page 28.

SERVICE DISRUPTIONS, DAY AFTER DAY

After phishing and scams, the third-largest category of incidents in 2024 was service disruptions, with an average of two per day. Malicious attacks did not always cause these; many resulted from hardware or software failures or even well-intentioned but flawed system updates by developers and administrators.

The most infamous software update from last year led to one of the most significant IT disruptions in history. In the early hours of 19 July, cybersecurity firm CrowdStrike released an update for its Falcon Sensor security software, which large organisations widely use to protect against malware and other threats. Unfortunately, the faulty update crippled 8.5 million Windows computers, causing them to crash with the notorious blue screen of death.

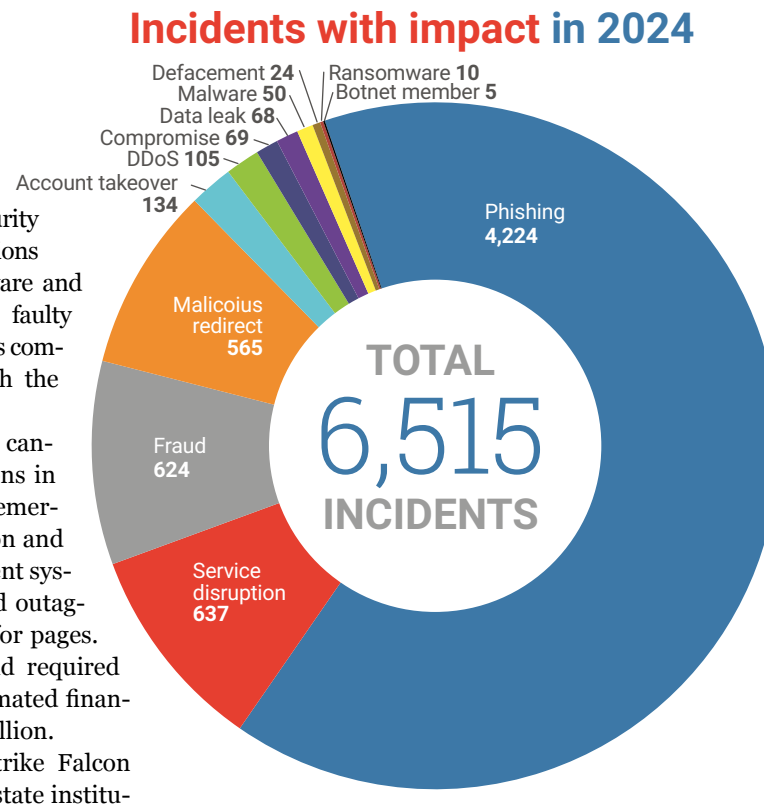
This resulted in more than 5,000 cancelled flights and service disruptions in banks from Brazil to New Zealand, emergency numbers, hospitals, television and radio stations, and even fuel payment systems at petrol stations experienced outages. The complete list could go on for pages. Restoring systems took weeks and required significant manual effort. The estimated financial damage quickly reached $10 billion.

Estonia was lucky, as CrowdStrike Falcon has relatively few users here. One state institution and one private company experienced only a few hours of disruption, and at Tallinn Airport, Ryanair check-ins had to be processed manually, causing minor delays. But overall, Estonia avoided the worst consequences.

After this unfortunate incident, many asked whether rushing software updates is really wise. Our answer remains yes: the risks of delaying updates are far greater. Read more about these risks on page 34.

While Estonia escaped the CrowdStrike disaster, a Cloudflare outage in September caused significant disruptions. On the third Monday of the month, Cloudflare's service failures affected nearly 200 public-sector websites that rely on RIA's protection against distributed denial-of-service (DDoS) attacks.

Mobile operators also faced network failures, which affected both data and voice services, including emergency calls. If your provider's network is down but you need to call emergency services, removing the SIM card from your phone allows it to connect to another operator's network for emergency calls.



There were also disruptions to national authentication services, including TARA, Smart-ID, Mobile-ID and the ID card. Most outages were short-lived or occurred overnight, when few people were attempting to log into online banking or sign digital documents.

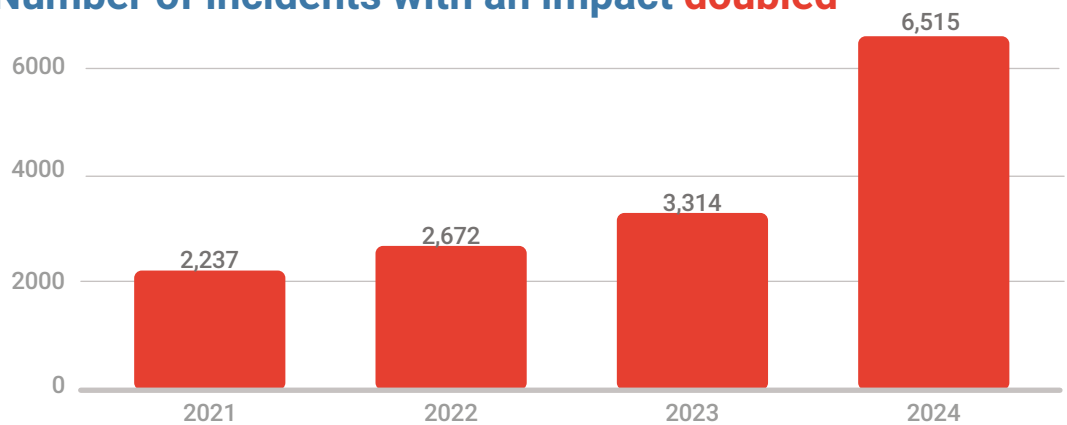
MORE DDoS ATTACKS, LESS DAMAGE

Websites and services can also be knocked offline by DDoS attacks, and last year left little room to breathe in this area. DDoS attack volumes have increased every year since Russia launched its full-scale invasion of Ukraine, and 2024 broke records for both attack numbers and scale. One four-hour wave of attacks targeting public-sector websites generated nearly three billion malicious requests. Under normal conditions, reaching this level of traffic would have taken more than 25 years.

However, the number of attacks is less significant than their impact – and in this regard, there is good news. In 2022, one in three DDoS

→

Number of incidents with an impact doubled



attacks succeeded in causing significant disruptions. By 2024, this figure had dropped to 18%. Some websites experienced short-term outages or slowdowns, but none of the attacks caused severe damage. Read more about DDoS attacks and their consequences on page 26.

DATA BREACH AFFECTS MORE THAN 700,000 PEOPLE

Last year, 68 data breach incidents were recorded in Estonia – nearly twice as many as in 2023. Some were relatively small in scale: for example, the exam information system's GitHub page accidentally contained real personal data instead of test data, making hundreds of people's details publicly accessible. Elsewhere, a waste management self-service portal accidentally displayed all customer transactions and personal identification numbers instead of just the user's own information.

In 2022, one in three DDoS attacks succeeded in causing significant disruptions. By 2024, this figure had dropped to 18%.

However, all these breaches pale in comparison to the cyberattack on Allium UPI, a company that manages loyalty card systems for Apotheka, Apotheka Beauty, and Pet City. Attackers gained access to this system and successfully stole nearly 700,000 personal identification numbers, more than 400,000 email addresses, and tens of thousands of phone numbers and home addresses. The stolen data originated from a backup of the customer database covering the years 2014–2020. Anyone affected by this breach should exercise even greater caution against phishing attempts and scams. Read more about this incident on page 18.

ATTACK ON CASH CIRCULATION

Unlike the pharmacy chain Apotheka, whose customer data was leaked, Hansab is not a household name, but its services are critical to nearly everyone. Hansab is responsible for filling Swedbank, Luminor and LHV ATMs, delivering pensions, issuing ID cards and passports in cooperation with the Police and Border Guard Board, and many other essential functions. In short, if its operations were to suddenly stop, almost everyone would feel the impact.

At midday on 1 March, Hansab's servers began unexpectedly rebooting. Within minutes, it became clear that something was terribly wrong. As an emergency measure, the company disconnected from the internet and isolated its network to prevent further damage. But the attack had already inflicted severe losses: the entire virtualisation environment had been

deleted. Hansab's CEO, Kristo Timberg, later described it as the attackers reaching the system's 'Holy Grail'.

Despite being a crisis for the company, it did not escalate into a national emergency. Cash supplies remained available – ATMs and shops were not emptied, and pension payments were delivered as expected at the beginning of the month. To keep services running, Hansab switched to manual operations, ensuring that ATMs remained functional, cash deposits from retailers were processed, and customer funds were credited.

This time, the impact was limited. However, longer-lasting payment disruptions or interruptions to cash circulation could be more severe. To prepare for such scenarios, it is advisable to keep enough cash on hand to cover at least a week's essential expenses.

CRIME AND PUNISHMENT

While some may assume that cybercriminals can operate anonymously with impunity, last year provided plenty of evidence to bust this myth, as multiple cases demonstrated that justice can catch up with cyber offenders.

In our previous cybersecurity yearbook, we covered a data breach at genetic testing company Asper Biogene, where attackers stole the personal data – including genetic and health information – of nearly 10,000 individuals.

A criminal investigation revealed that a four-person group spent two months persistently working to infiltrate the company's systems. First, they identified a security vulnerability that allowed them to access usernames and encrypted passwords. Next, they decrypted an employee's password, used it to log into the system and installed malware. This granted them access to sensitive health records, which they downloaded before demanding a €45,000 ransom.

The group's leader was Vladislav Rybakov, a Russian citizen, whose travel options have since become severely restricted. Due to his role in the Asper Biogene attack, he is now an internationally wanted criminal.

Following the breach, Estonia's Data Protection Inspectorate launched a parallel investigation, finding serious shortcomings in Asper Biogene's information security practices. As a result, a fine of €85,000 was imposed, though, at the time of writing, the decision had not yet entered into force.

In 2020, Estonian government bodies suffered a major cyberattack, during which 350 GB of data was stolen from the Ministry of Economic Affairs and Communications; hackers also accessed records on 10,000 COVID-19 patients from agencies under the Ministry of Social Affairs. Investigations by the Estonian Internal Security Service (KAPO) and the National Criminal Police eventually led to three men, all of whom were working for Russia's military intelligence (GRU) at the time of the attack: Colonel Yuri Denisov, commander of GRU Unit 29155, Nikolay Korchagin and Vitali Shevchenko. These individuals are now also internationally wanted. Read more about this case on page 20.

To prepare for such scenarios, it is advisable to keep enough cash on hand to cover at least a week's essential expenses.

Last year, the Harju County Court sentenced a young man from Tallinn to prison for selling phishing toolkits and providing guidance on how to carry out cyberattacks. His tools, which he sold using the Telegram messaging app, were explicitly designed to bypass two-factor authentication. This allowed criminals to steal victims' login credentials and gain access to Microsoft 365, PayPal, Google, Yahoo, Dropbox, Binance and other online accounts.

As for the perpetrators of the Allium UPI and Hansab attacks, that remains an open question. Hopefully, in a future edition of this yearbook, we will be able to report on their identification and prosecution. Until then, stay vigilant in cyberspace!

UKRAINE WAR: cyberattacks move closer to the frontline

On 19 November last year, 1,000 days had passed since Russia's full-scale invasion of Ukraine began. The battle in cyberspace, which supports military objectives, has lasted even longer.

The number of critical, high-impact incidents declined in 2024, but the total number of incidents and attacks targeting government institutions and local authorities increased. Cybercrime for financial gain, state-sponsored groups targeting critical infrastructure and covert cyber intelligence activities have continued unabated.

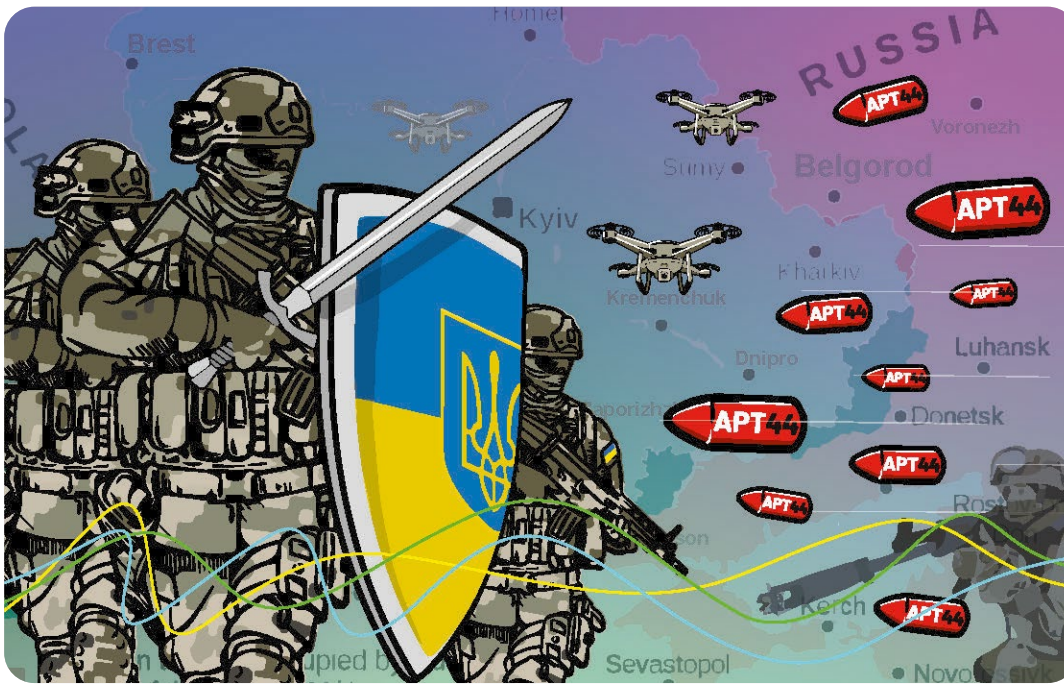
CYBERATTACKS SUPPORTING MILITARY OBJECTIVES

A notable trend has been the increasingly systematic use of cyberattacks to support military objectives. Cyberattacks against the security and defence sectors increased compared to the previous year, and Russia intensified efforts to gather intelligence via Ukrainian military personnel's devices.

Analysts from the cybersecurity company Mandiant reported on the consistent activities by the Russian state-sponsored group APT44, which hacked into the phones and other stolen devices of fallen Ukrainian soldiers to extract conversations and data. Enemy cyber activities aimed at monitoring troop movements and logistical chains have, in some cases, moved directly to the frontline.

Both military personnel and civilians are increasingly targeted through communication apps. Malware is distributed through these apps for financial gain and intelligence purposes, while compromised applications can also reveal the locations of users, such as military units.

As a result, Ukraine's National Security and Defence Council decided in September to ban the use of Telegram on devices used by government agencies, the defence sector and critical infrastructure employees. Kyiv National University followed suit by prohibiting Telegram for its staff and advising students to limit its use.



Despite these restrictions, Telegram remains one of the primary communication and news platforms in Ukraine. Even after the restrictions, exceptions were made for officials whose roles require ongoing public interaction.

A GRIM DECEMBER

As in 2023, the most impactful cyberattack on Ukrainian citizens occurred in December. This time, nearly 60 national databases and registries were targeted, disrupting essential digital services, including issuing birth or death certificates, registering marriages, handling real estate transactions, inheritance processes and various other notarial services.

Several services in the state-run Diia app were also affected, as they could not connect to the necessary databases. At the time of writing, details about the attack remain scarce, but Ukrainian authorities suspect the involvement of Russian military intelligence.

While services had to revert to paper-based processes, some were recovered by the start of the new year, and further disruptions in other services are expected to be temporary.

This attack underscores that the aggressor waging a full-scale war of conquest continues to target and attempt to disrupt Ukraine's critical civilian infrastructure.

What is APT44?

- APT44 (also known as Sandworm) is a technically sophisticated hacker group linked to Russian military intelligence.
- It is one of the main state-sponsored cyber threats in Ukraine, though it operates elsewhere as well.
- The group is active in disrupting critical infrastructure, conducting cyber intelligence and executing influence operations.
- In 2015 and 2016, it attacked Ukraine's power grid, causing outages affecting hundreds of thousands of people.
- In 2017, APT44 deployed the NotPetya malware against Ukrainian networks. The malware quickly spread worldwide, causing an estimated $10–11 billion in damages.
- In spring 2024, the group targeted Ukraine's energy and water infrastructure, but Ukrainian efforts successfully thwarted the attack.

SSSCIP CHIEF: Russia operates more covertly in cyberspace

We learn about the cyberattacks thwarted in 2024 through an interview with Brigadier General **Oleksandr Potii**, head of Ukraine's State Service of Special Communications and Information Protection (SSSCIP) and a close partner of CERT-EE.

How have Russian cyberattack capabilities evolved in 2024? What changes have you observed compared with the previous year?

In 2023, we saw destructive cyberattacks by Russian hacker groups targeting IT and telecommunications companies. At least 11 internet service providers suffered from such attacks, culminating in the cyberattack on Kyivstar in December 2023. These attacks were accompanied by data leaks and publications on Russian social media networks.

In 2024, Russia gradually shifted away from publicising its cyberattacks, as it focused instead on cyber intelligence operations targeting systems linked to war and politics, aiming to remain undetected for as long as possible. The main targets were Ukraine's security and defence sectors, as well as companies directly supporting them.

There was also a significant increase in the activity of Russian financially motivated groups in 2024, including targeted cyberattacks on large organisations and various fraud schemes. We believe these criminal hacker groups operate under the direction or approval of the Russian government, as some engage in both financial theft and cyber espionage.

Have you observed AI-enabled cyberattacks from Russia? Has the broader use of AI led to any significant changes?

AI is already being used in cyberattacks, for example, to generate phishing emails in Ukrainian or to facilitate interactions between hackers and victims through messaging apps or email. The use of AI components will undoubtedly increase further.

In 2024, there was only one widely publicised attack on Ukraine's critical infrastructure – the December attack on state registries. This seems to suggest your defences have been largely effective. Which critical sectors faced the greatest threats last year?

Indeed, 2024 ended with a high-profile attack on the Ministry of Justice's registries. However, attempts to target critical infrastructure were detected throughout the year.

For example, in March, preparations by UAC-0002 (also known as Sandworm) for



Photo: SSSCIP

Oleksandr Potii

cyberattacks were uncovered. These attacks aimed to disrupt the stable operations of approximately 20 energy, water and heating companies across ten Ukrainian regions. The attacks were attempted through compromised supply chains, specifically through Ukrainian companies developing specialist software for industrial systems.

Thanks to operational measures to detect and respond to these preparations, the attacks were thwarted. Interestingly, the timing of these activities coincided with missile strikes against Ukrainian infrastructure in the spring of 2024, which suggests the cyberattacks were intended to amplify the impact of physical strikes.

Another incident involved the discovery of malware called FrostyGoop at a Ukrainian energy-sector facility. It was specifically designed to target industrial systems. This demonstrates that Russian actors continue to refine their tools and plan further cyberattacks on critical infrastructure.

How would you characterise Russian hacktivists attacking Ukraine? Are they more of a nuisance or a serious threat?

We cannot say that Russian hacktivists significantly contribute to the cyber war compared with Russia's well-known state-sponsored hacker groups. However, it is important to note that in a totalitarian state like Russia, there are no truly independent hacktivists. To some extent, they are all controlled and work for the Russian government. A growing concern is that these hacktivists serve as a reserve pool for Russia's intelligence services, which could eventually involve them in more complex cyberattacks.

Now that North Korea is increasingly involved in the conflict, have you seen more cyberattacks originating from that region?

So far, we have not identified any cyberattacks linked to North Korean hacker groups. Still, we cannot rule out the possibility of their involvement in future cyber operations, as Russia's collaboration with North Korea is growing by the day.

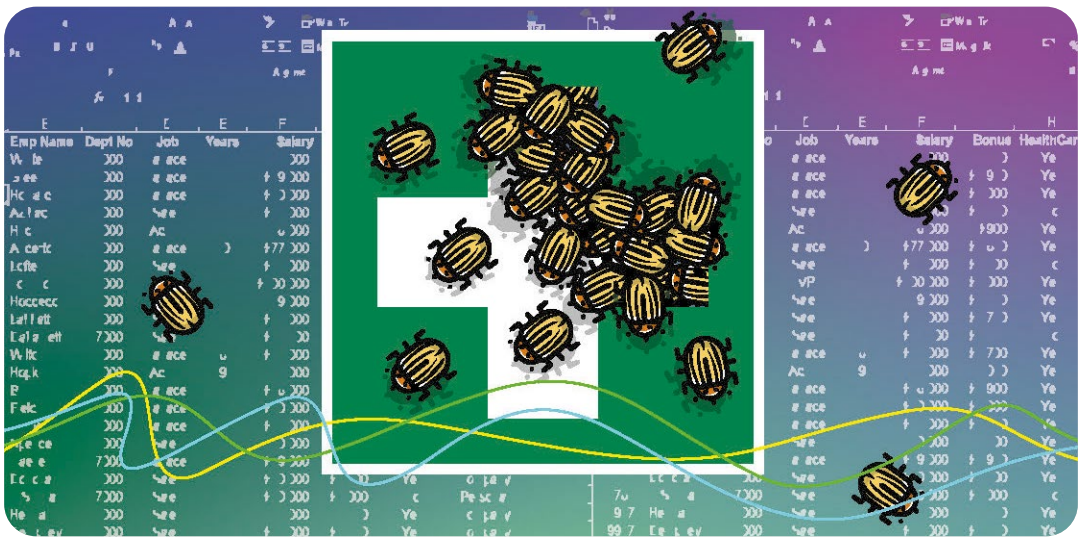
What do you foresee as the biggest cyber threats in 2025, both for Ukraine and globally?

In 2025, we expect an increase in cyber intelligence operations targeting Ukraine's security and defence sectors, as well as its defence industry. Given Russia's preparations for a potential war with NATO, cyber intelligence operations against military organisations in NATO member states will also intensify.

Destructive cyberattacks on critical infrastructure will become more frequent and will likely coincide with physical sabotage activities, which Russia has already initiated against NATO member states.

Given Russia's preparations for a potential war with NATO, cyber intelligence operations against military organisations in NATO member states will also intensify.

We are also seeing a growing number of financially motivated cyberattacks from Russia against Ukrainian commercial enterprises. This trend is expected to continue and will likely spread to NATO countries. The use of AI in conducting such cyberattacks and the cooperation between cybercriminals and the Russian government, which shields them from international prosecution, will further exacerbate the threat.



LESSONS from a massive data leak

At the beginning of 2024, criminals breached a server of Allium UPI, stealing data on the customers of Apotheka, Apotheka Beauty and Pet City. The leak included nearly 700,000 personal identification codes, over 400,000 email addresses, and tens of thousands of phone numbers and home addresses. Why and how did this happen?

The Estonia-based company Allium UPI, which operates in the pharmacy and healthcare product sectors in Estonia, Latvia and Lithuania, reported in February 2024 to both the Estonian Police and Border Guard Board and the Information System Authority's incident handling unit (CERT-EE) that their loyalty card system had been illegally accessed. The intruders downloaded data on the customers of Apotheka, Apotheka Beauty OÜ and PetCity OÜ, including personal identification codes, purchase data and contact information.

The Police and Border Guard Board's criminal investigation revealed that nearly 700,000 personal identification codes, over 400,000 email addresses, around 60,000 home addresses and approximately 30,000 phone numbers

were unlawfully downloaded from UPI's database. In some cases, it was possible to identify over-the-counter medications and other pharmacy products purchased, though prescription medication data was not accessible. Since the loyalty programme did not store passwords, bank card information or other financial details, these were not compromised. The data came from a backup of the customer database containing records from 2014-2020.

WHY DID THIS HAPPEN?

Cyberattacks with serious consequences often begin with the takeover of an employee's user account. Criminals can obtain usernames and passwords through methods such as malware, which might be downloaded to an employee's computer using a malicious email attachment or pirated software from an untrusted source.

Two-factor authentication should be implemented to prevent criminals from immediately accessing systems with a leaked password. Furthermore, only information systems and services that absolutely must be online should have internet access, and all such systems should be secured behind a VPN or similar protective solution.

Given the highly international nature of cybercrime, leaked data can circulate for years among different countries and groups, who will be able to use it to carry out various cyberattacks.

DATA IS PERSONAL PROPERTY

This incident once again brought the issue of protecting sensitive personal data into the public spotlight in Estonia. People increasingly trust their data to a growing number of service providers, expecting these providers to take their data protection responsibilities seriously. Unfortunately, this is not always the case, but similar incidents in recent years have raised awareness among both service providers and individuals, encouraging better preparedness and action.

As customers, we should critically assess the sharing of our personal data, including for loyalty accounts. A small discount or slightly more convenient service may not be worth the risk.

Lessons from the eye of the storm

'An experience like this is a cold shower,' recalls Marika Pensa, a member of the management board at Allium UPI.

Last winter, criminals stole a backup of the Apotheka customer database. Following this unfortunate incident, we, as a service provider, have placed even greater emphasis on system security. Criminals never rest, and they exploit any weakness that may have escaped the heightened attention of system administrators.

The first lesson is simple: ensuring security is an ongoing process that never ends. It's like riding a bicycle; you must keep moving to stay upright.

For a company that has become a victim or target of a cyberattack, such an experience is a cold shower, but also a reminder and an opportunity to reassess its systems. Cybersecurity is no longer just something described as "nice to have".

Another lesson from this incident is that criminals don't see the world as divided into business, government, customers, or other neatly defined boxes. Effective action against crime can only be achieved through unified collective defence involving individuals, companies, governments and others. That's why we are very happy about the effective cooperation we've had with Estonian government agencies, from the Police and Border Guard Board to the Information System Authority and the Data Protection Inspectorate. We all understand that we are on the same side of the front line, with international criminals on the other side. We hope the perpetrators of this crime will be apprehended and held accountable.

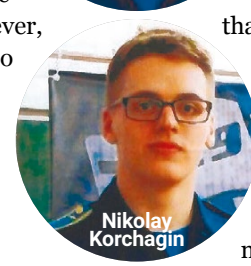
The fight against cybercrime requires continuous and growing attention from all of us. The question is not whether a cyberattack will happen but when, on what scale and in which area. There are no bulletproof individuals or systems, but robust defences against external attacks can save lives and protect data.

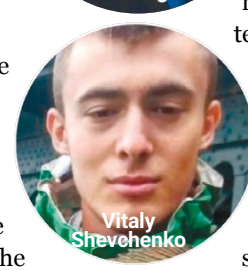
RUSSIAN INTELLIGENCE ramps up cyber pressure on the West

A thorough investigation linked several cyberattacks against Estonian government agencies in 2020 to Unit 29 155 of Russia's military intelligence (GRU).

The case began to unfold four years ago when an employee of the Estonian Ministry of Economic Affairs and Communications noticed unusual anomalies on their computer. Initially, they suspected malware that was widespread in Estonia at the time. However, when cleaning the computer failed to resolve the issue, the employee reported it to CERT-EE, the incident handling unit of the Information System Authority.


Yuri Denisov


Nikolay Korchagin


Vitaly Shevchenko

THE PROBLEM WAS BIGGER THAN IT SEEMED

It quickly became clear that the issue was far more extensive. A backdoor had been built into the ministry's systems, allowing the exfiltration of large amounts of data – 350 gigabytes in total. While classified state secrets were not compromised, the attackers gained access to a significant amount of sensitive internal information, including strategic documents and working papers, personnel details, and correspondence with businesses.

Tracing the cyber footprint revealed that attacks with a similar modus operandi had targeted other government institutions and companies, including the Ministry of Foreign Affairs and the Health and Welfare Information Systems Centre (TEHIK). While hackers extracted only public data from the ministry's web servers, in TEHIK's systems, they accessed the personal information of around 10,000 individuals infected with COVID-19.

The investigation, conducted by the Estonian Internal Security Service and the National Criminal Police, identified three suspects who were serving in the GRU at the time of the


Cadet Blizzard
CYBER ATTACK

attacks: Colonel Yuri Denisov, head of Unit 29 155, and his subordinates Nikolay Korchagin and Vitaly Shevchenko. In autumn 2024, Harju County Court placed the suspects, who reside in Russia, under international arrest warrants and detention orders in absentia at the request of the Estonian Prosecutor's Office.

This marks the first time Estonia has officially attributed state-sponsored cyberattacks to specific individuals. The attribution of cyberattacks is coordinated by the Ministry of Foreign Affairs and aims to promote responsible state behaviour in cyberspace and hold actors accountable when necessary.

ALLIES OF UKRAINE TARGETED

At the same time, Estonia and nine other countries concluded Operation Toy Soldier, which linked Unit 29 155 to numerous cyberattacks against Ukraine and its NATO and EU allies. As part of this effort, the United States offered a $10 million reward for the capture of six Russian citizens, including Denisov and Korchagin, who were also wanted by Estonia.

Unit 29 155 is reportedly the third GRU unit to develop its own cyber capabilities. According to a US indictment, the unit's primary focus in recent years has been on Ukraine. In early 2022, a month before Russia's full-scale invasion, the unit launched the destructive WhisperGate malware attack, which targeted the Ukrainian government and law enforcement agencies, as well as emergency services. The attack employed destructive malware aimed not at taking control of systems but at rendering them entirely inoperable. Since the malware was disseminated via the services of a US-based company, the perpetrators could also be prosecuted in the United States.

Globally, the unit's primary objective has been to disrupt international aid to Ukraine, according to US government data. In NATO member states and other countries in Europe, Central Asia and Latin America, the unit has targeted government institutions and critical infrastructure, including banking, healthcare, transportation and energy sectors. Its activities have included defacing websites, mapping infrastructure and stealing data, which they subsequently either sold or leaked. Microsoft has codenamed this GRU cyber unit Cadet Blizzard, noting that it has also targeted IT service providers and software developers in Ukraine and other European countries to gain access to public-sector institutions through their supply chains.

The methods employed by this GRU cyber group are not necessarily sophisticated or advanced. Both in Estonia and elsewhere, they have exploited known security vulnerabilities, such as those in email and web servers, and used stolen user credentials to access their targets. The unit has leveraged tools widely used in the cybersecurity community to identify and exploit vulnerabilities, exfiltrate data, and cover their tracks.

LESSONS FROM THE INCIDENT

In recent years, the global cybersecurity landscape has become increasingly complex due to rising geopolitical tensions and new technological developments, which state-sponsored

Cyber operations are part of Russia's hybrid warfare

According to Margo Palloson, Director General of the Estonian Internal Security Service (KAPO), the objectives of GRU's cyber cell, Unit 29 155, include gathering intelligence, causing reputational damage through the theft and leak of sensitive information, and systematic sabotage by destroying data and computer systems. While the GRU unit was officially linked to the 2020 cyberattacks, various Russian cyber intelligence units carry out operations against Estonia and other nations on an ongoing basis.

The tools of Russian intelligence increasingly blend physical and cyber capabilities, making it likely that information obtained through cyberattacks could be used in physical operations. According to Russia's military doctrine, cyber operations are a crucial component of hybrid warfare. Regardless of the methods employed, Russia's hybrid attacks aim to impose its will on other nations, sow instability, instil fear and create confusion.

cyber groups have exploited to expand their activities.

In response, Estonia has significantly increased its investments in cybersecurity and the protection of critical infrastructure. Central to this effort is the services provided by the Information System Authority, which helps government agencies secure their networks, continuously search for vulnerabilities, and notify government institutions and businesses about identified issues. If an incident does occur, CERT-EE experts are available to investigate the causes and assist in resolving the situation.

Although most private companies in Estonia are not legally required to report cyber incidents, doing so is highly recommended. Reporting incidents enables CERT-EE to gain a better overview of Estonia's cyber landscape and improve the protection of both businesses and the national system as a whole. It also helps identify the activities of state-sponsored cyber actors.

State-run cyber units are characterised by persistence: if an attack fails once, it can be expected to be attempted again. Government institutions and critical infrastructure companies are undoubtedly at the highest risk, but firms providing services to them – such as IT or accounting companies – are also vulnerable to supply chain attacks. Often, similar attack patterns are used against multiple organisations simultaneously, making every piece of information vital for understanding the bigger picture. An anomaly that might seem insignificant at first could, upon closer examination, turn out to be a serious cyberattack.

Ultimately, each organisation is responsible for protecting its own systems and much depends on how seriously its leadership prioritises information security. If necessary, the Information System Authority's supervision department can remind organisations of the importance of cybersecurity. This department has significantly expanded its reach, having initiated nearly 150 supervisory review proceedings over the past three years. The work is mainly preventive: instead of reacting solely to identified problems, the department proactively monitors the situation in critical institutions and companies based on threat forecasts.

How to protect yourself from cyber espionage

As state-sponsored cyber groups often employ the same methods and tools as financially motivated cybercriminals, general cybersecurity recommendations remain relevant. However, some specific aspects should be kept in mind:

- **Preserve system logs.** Retaining system logs is critical for detecting any cyberattacks. Record as much information as possible (e.g. firewall logs) to understand what attackers did and how they did it. However, logs are only useful if they can be analysed effectively and threats are acted upon promptly. Remote access solutions and the accounts they use should be monitored with particular care.
- **Segment internal networks.** Depending on organisational needs, internal networks should be divided into segments, with access permissions granted strictly on a need-to-know basis. Administrators must use separate accounts – one with user-level permissions for daily tasks and another with elevated privileges only when necessary. Passwords should never be reused across systems, and two-factor authentication should be implemented wherever possible.
- **Modernise systems.** Keep centralised management systems up to date and phase out outdated software and hardware. While an upfront investment to eliminate legacy systems might seem high, it can prevent much greater damage in the long run.
- **Address supply chain risks.** When using services provided by external partners, consider supply chain vulnerabilities. Regularly audit external partners' access to your systems and grant them only the minimal permissions required for their work.

For more detailed technical guidance, consult recommendations from the US Cybersecurity and Infrastructure Security Agency (CISA) here.

PHISHERS caught on the hook

The international police operation **PhishOFF** shut down LabHost, one of the world's largest platforms used by phishing scammers, with over a million people impacted. The Estonian police played a key role in preparing the raid.

Years ago, simple scams like "Nigerian letters" offering vast sums of money were the subject of jokes. Today, however, cyber fraud has taken a giant leap forward, often orchestrated by sprawling international networks and organised crime.

These operations function like well-oiled machines with distinct roles: some criminals breach systems, others create virtual environments such as phishing websites, while another group devises ways to quickly and effectively drain bank accounts using stolen data. Finally, specialist teams help launder the illicitly obtained funds. Dedicated platforms now allow criminals to purchase phishing services, denial-of-service attacks, ransomware and other malware as a service.

OVER A MILLION VICTIMS

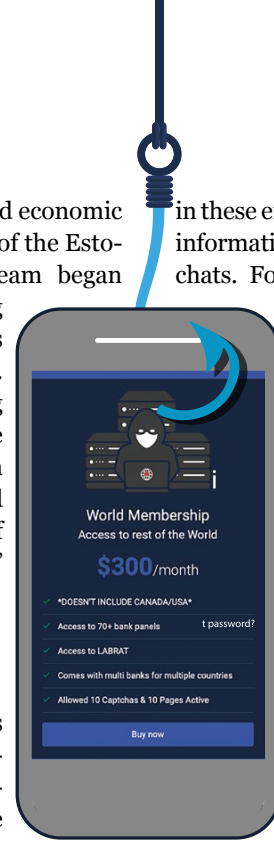
One of the largest operations of its kind, LabHost, focused specifically on facilitating phishing scams. It was dismantled in April 2024 during the international police operation PhishOFF, with significant contributions from the Estonian police. Coordinated by Europol, the five-day raid resulted in the arrest of 37 organisers of phishing scams worldwide. The operation involved 18 countries, primarily in Europe, but also included the United States, Canada, Australia and New Zealand.

Launched in 2021, LabHost was a public platform offering pre-built fake websites, phishing systems and distribution solutions (via SMS or email) while also selling stolen data collected on its platform. Thousands of regular criminal clients purchased access to phishing packages to execute their schemes. These packages included fake websites mimicking major banks and services across dozens of countries, enabling fraudsters to steal authentication details and money from victims' bank accounts.

Higher-tier packages cost between €230 and €350 per month, with quarterly and annual subscriptions also available. Payments were made in cryptocurrency, and LabHost reportedly earned around €1 million from its services, but the financial damage to victims was far greater. The platform handled the most tedious and time-consuming aspects of cybercrime; its administrators offered technical support to criminals through a dedicated Telegram channel.

The international investigation uncovered at least 66,000 websites used by nearly 10,000 criminals to steal data or money. Globally, over a million people have fallen victim to scams that have been executed through this platform. LabHost facilitated the theft of 480,000 bank card details, 64,000 PIN codes and over a million passwords. Stolen funds were transferred between various bank accounts to obscure their origins before being withdrawn as cash. In Estonia alone, up to 30 criminals used LabHost for phishing attacks, with around 10 of the most active offenders arrested in different countries.

Hannes Kelt, head of the cyber and economic crimes unit at the North Prefecture of the Estonian police, explained that his team began investigating a wave of phishing links exploiting the names of banks operating in Estonia a few years ago. "Collecting evidence and analysing the data led us to LabHost. We brought in other countries, which also launched investigations, and the result was the closure of one of the largest platforms of its kind," Kelt said.



CRIMINALS DETERRED WITH THREE SOFTWARE TOOLS

The unit led by Hannes Kelt was tasked with discouraging and deterring criminals operating on the LabHost platform; the team used three software tools. The first tool was designed to neutralise all phishing websites actively used for scams. After months of information gathering and analysis, all fraudulent environments and the thousands of associated phishing sites were shut down in April 2024.

Simultaneously, raids led to the arrest of dozens of crime organisers. However, the platform has been used by thousands of lower-level criminals worldwide. To target these individuals, experts from the North Prefecture developed a second programme resembling a social media or content-sharing platform.

Much like year-end summaries sent by commercial platforms ("2024 Wrapped"), which show users the pictures they have shared, the posts they have made, or the music they have listened to most, 700 of the most active scammers using fraudulent platforms received a similarly detailed report from the police about their activities. At the end of the report was a recommendation to contact the police and confess their crimes as soon as possible – many did. Another 1,500 less active criminals received written summaries of their activities, reminding them that operating on fraudulent platforms does not guarantee anonymity or protection.

The third tool was used within the criminals' communication platforms. A chatbot operating in these environments was taken over, and police information was disseminated through their chats. For example, criminals received videos and messages showing arrests and examples of evidence gathered from the platform, aiming to amplify the police's message and demonstrate that even encrypted communication platforms do not provide complete anonymity.

"This type of deterrence is particularly effective for less experienced criminals to nudge them back onto the right path early on. Overall, the operation was very successful, as even LabHost's key figures acknowledged in the end, warning their clients themselves and advising them to go into hiding and destroy their devices," Kelt explained.

THE FIGHT CONTINUES

Kelt emphasised that international operations of this scale require excellent cooperation and coordination. "Through joint efforts, we shut down a platform that enabled thousands of scammers to operate. Unfortunately, this was not the only such platform, and police efforts to stop fraudsters continue. Fraud is a global crime, and even shutting down a major platform doesn't provide a permanent solution, as criminals remain highly motivated to develop and use new methods of fraud."

CERT-EE, the Information System Authority's incident handling unit, identifies hundreds of phishing and scam sites every month. CERT-EE blocks access to these sites, notifies web hosts and shares information with its international partners. Over recent years, tripartite cooperation with the police and banks operating in Estonia has become so effective that detected phishing sites can now be taken down in just minutes, halting data theft swiftly.

In recognition of its contributions to the preparation of PhishOFF, the Cyber and Economic Crimes Unit at the North Prefecture of the Estonian Police and Border Guard Board received Europol's award for the most innovative police operation in 2024.

DDoS ATTACKS more noise, less impact

Last year, CERT-EE registered an unprecedented number of distributed denial-of-service attacks, but effective defence measures reduced the proportion of attacks that had a significant impact. A new trend saw attackers shift their focus to name servers.

In 2024, CERT-EE registered 580 distributed denial-of-service (DDoS) attacks. This was 93 more than in 2023 and 50% more than in 2021 and 2022 combined.

Just as attackers are constantly seeking new ways to cause maximum harm, CERT-EE continuously improves its DDoS defences to counteract them. The more attackers target the websites protected by CERT-EE, the more effectively CERT-EE's DDoS defence measures can be enhanced.

As a result, despite the alarmingly high number of attacks, the proportion of impactful ones dropped to just 18%. This represents significant progress compared to the previous year, when that figure was 27%.

What is a DDoS attack?

A distributed denial-of-service (DDoS) attack is a cyberattack in which a large volume of malicious requests is directed at a target's servers to overload them and render the service inaccessible to users. Since most DDoS attacks against Estonia are politically motivated, they typically target services whose disruption would affect the largest number of people, such as national e-services, banks and the transport sector.

TARGETING NAME SERVERS

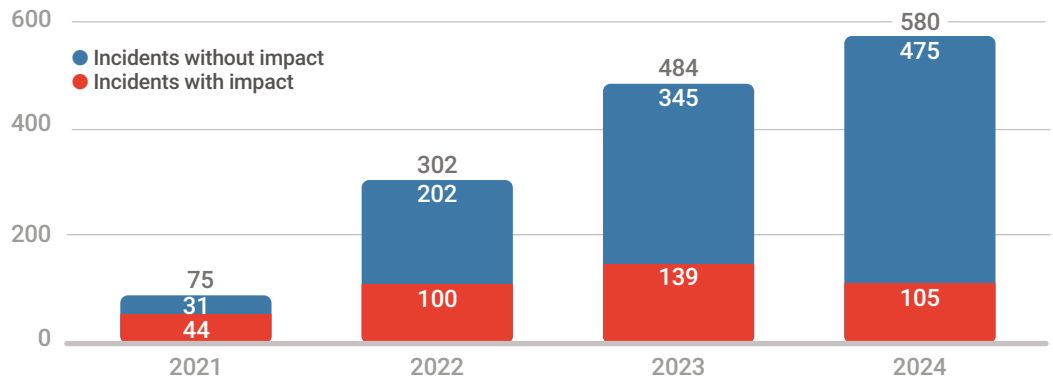
One of the most notable trends of 2024 was attackers increasingly targeting name servers rather than web servers.

A name server translates IP addresses into domain names, allowing users to type google.com instead of remembering a numeric sequence like 142.250.189.206. While name servers do not host web content themselves, they help users locate it. If attackers succeed in disabling name servers through a denial-of-service attack, users cannot access websites, even if the web servers are functioning normally.

As Estonian organisations' web servers have faced constant attacks over the years, they are now better protected. This forced attackers to change tactics, turning their focus to name servers, which are somewhat more complicated to defend.

This wave of attacks began in May 2024, when the share of denial-of-service attacks targeting Estonian organisations' name servers jumped from the usual 3-8% to 69%. At the

DDoS attacks increased, but impact dropped



same time, attacks against web servers decreased. By the end of the year, attacks on name servers accounted for an average of 90% of all denial-of-service attacks registered by CERT-EE.

This trend clearly shows that attackers adapt to security measures and constantly seek new vulnerabilities to exploit. When systems critical to the functioning of the internet are targeted, the consequences of attacks can extend far beyond disabling individual websites.

This shift underlines the need for institutions and companies to invest more heavily in protecting name servers, which form the backbone of the internet.

THE VOLUME AND SCALE OF DDoS ATTACKS CONTINUE TO GROW

Due to ongoing geopolitical tensions, distributed denial-of-service attacks are expected to increase further in 2025. These attacks will remain a popular tool for both state-sponsored groups and independent hacktivists. The rising popularity of this type of attack has led to the emergence of platforms and service providers that offer DDoS attacks for hire, making them more powerful and accessible even to less experienced cyber criminals. This, in turn, raises the overall threat level in cyberspace.

It is also likely that attackers will increasingly target components critical to internet functionality, such as name servers, cloud services and authentication services that many other services rely on. With the help of artificial intelligence and machine learning, distributed denial-of-service attacks are becoming more dynamic, allowing them to be adjusted in real-time to bypass defence mechanisms and complicate countermeasures.

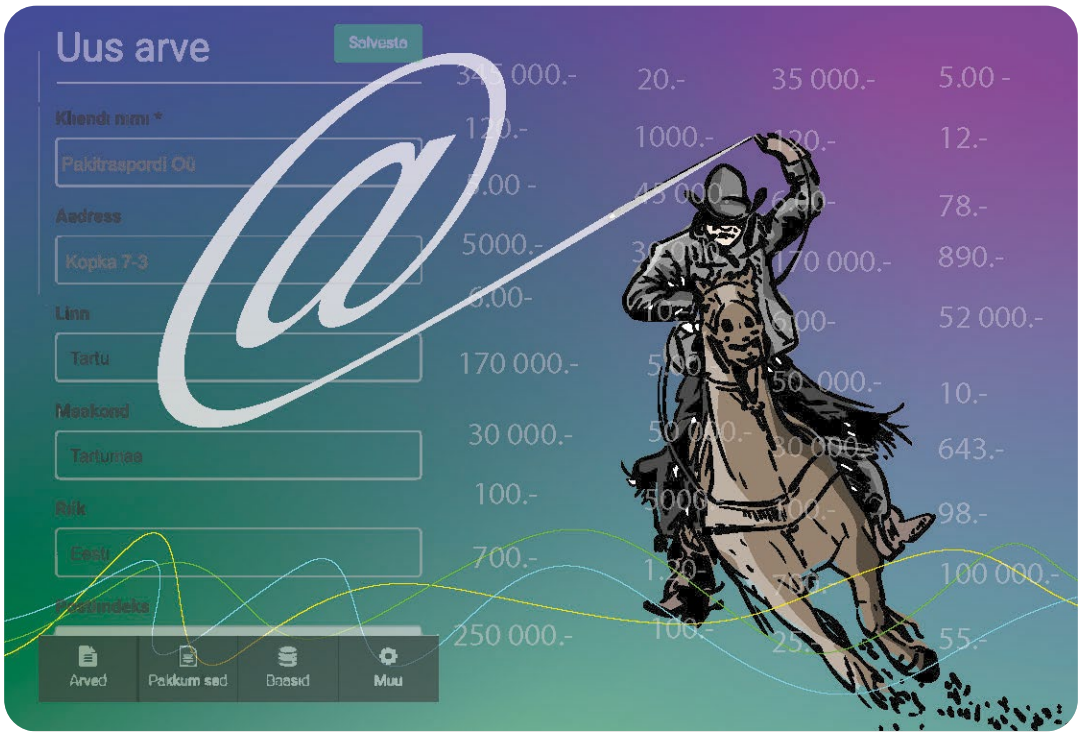
26 years' worth of traffic in four hours

In March, Estonia's public sector faced an unprecedented wave of distributed denial-of-service attacks. Over a span of just four hours, attackers directed nearly 2.8 billion malicious requests at the websites of three institutions. Under normal circumstances, generating such a volume of traffic would have taken approximately 26 years.

The wave of attacks was carried out by two Russian hacktivist groups, targeting 16 Estonian government institutions.

Despite the unprecedented scale of the attacks, the impact on the three targeted websites was minimal.

Although the attackers managed to produce a massive volume of malicious requests, the attacks themselves were not particularly sophisticated. Thanks to DDoS protection measures and CERT-EE's active response, most of the requests never reached their intended targets. Out of the other 13 targeted websites, only three experienced brief disruptions, while the remaining 10 were unaffected by the attacks.



FRAUDSTERS made off with millions

Despite awareness campaigns by the Estonian Police and Border Guard Board, the Information System Authority and other organisations, the final figures for last year sadly confirm that it was a successful year for fraudsters.

In 2024, CERT-EE recorded 624 significant fraud incidents, compared to 546 incidents recorded in 2023. During the first 11 months of the year, Estonian citizens lost €7 million to fraud, according to data from the Police and Border Guard Board. Since many cases go unreported, the actual losses are likely much higher.

But why do so many fraud attempts succeed? There are several factors. First, scammers have become increasingly sophisticated, and their

messages appear more convincing. Second, in today's fast-paced world, people often multitask and let their guard down. Third, with more individuals shopping online frequently, they are often waiting for deliveries, which increases the likelihood of them mistaking a scammer's message for a genuine notification about a package.

BUSINESSES PLAGUED BY INVOICE FRAUD

Invoice fraud has become a relatively common type of scam in which fraudsters send a fake invoice to an organisation under the guise of a legitimate business partner. The phoney invoice usually differs only in the payment account details, making the fraud easy to overlook. The recipient unknowingly transfers money to the fraudsters, while the actual partner continues to wait for payment.

This type of fraud can be difficult to detect, as criminals often hijack ongoing correspondence, leading the victim to believe they are still communicating with their business partner. However, changes to account details, which are not a common practice, should serve as a warning sign.

In November, we received reports about four cases of invoice fraud with damages totalling nearly €300,000.

In one case, an Estonian company transferred over €170,000 to an account controlled by fraudsters. The criminals had compromised the company's email account and monitored correspondence with a supplier. At the right moment, they sent an invoice in the supplier's name with altered account details, and the recipient made the payment.

In another case, a state-owned company fell victim to fraud when an invoice sent to its general email address appeared legitimate. The amount matched expectations, but the bank account details had been changed. The company transferred nearly €30,000 to the fraudsters, only discovering the fraud when the real business partner, who had not received the payment, asked for a payment confirmation.

A third case involved an Estonian company purchasing a new car. Over the course of a month, the company corresponded with a German car dealer, finalised the contract and transferred the payment according to the provided bank details. When it came time to deliver the car, it was revealed that the bank account belonged to fraudsters, and nearly €60,000 had gone to the wrong account. The criminals had hijacked the correspondence and altered the payment details.

In another instance, an industrial company fell victim to invoice fraud. The fraudster intercepted correspondence at the right moment and issued a fake invoice. Since the company →

How to avoid invoice fraud

- Raise awareness about invoice fraud. Everyone in your organisation who approves invoices should understand the nature and signs of such fraud. As a starting point, share the post published on RIA's blog (ria.ee/blogi/levivad-arvepet-tused-kontrolli-enne-kui-maksad) and explain the issue to your employees.
- Agree on an invoice approval procedure. For example, establish a rule that if invoice details, such as bank account information, have changed, the sender must be contacted through an alternative channel, such as by phone. Be sure to use a known contact number rather than the one listed on the invoice, as fraudsters may replace genuine contact information with their own.
- If you or your accountant suspect that a payment has been made to the wrong account, contact your bank immediately. In the age of instant payments, reaction time is limited, but prompt action may allow the bank to reverse the transfer.
- If you identify or suspect a fake invoice sent in the name of a business partner, contact the partner immediately. Use a different channel from the one through which the invoice was received. Acting quickly in this way can help uncover the problem before it reaches the next victim.

was due to pay its next instalment, everything seemed legitimate, and the nearly identical invoice was paid. The accountant did not suspect that the payment details had been altered.

THE CRYPTO BOOM BROUGHT NEW SCAMS

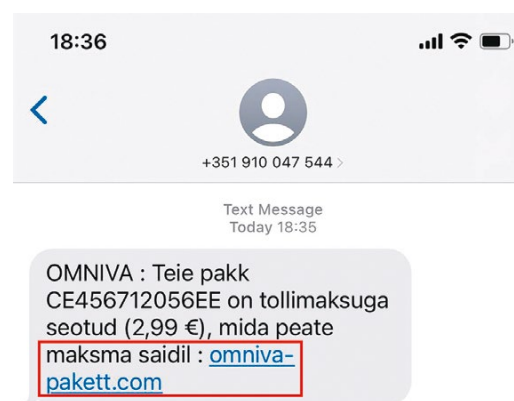
Fraud involving cryptocurrency is becoming increasingly common. Since the field is often associated with promises of quick and easy profits, scammers have started exploiting the trust of unsuspecting individuals. The schemes vary, but the pattern is often the same: a person is offered an opportunity to earn money and is guided through making an initial deposit on a cryptocurrency trading platform. The process typically starts with smaller amounts, such as €250, transferred to the platform. After the initial payment, the person is shown how much profit they are supposedly making. They withdraw the earnings, which builds trust and encourages reinvestment, this time with a larger sum. The second time, the person transfers a significantly higher amount to the scammers' account. Later, they are informed that additional fees are required to access their funds. They pay even more, but ultimately, they are unable to retrieve either the initial amount or the extra money.

In some cases, these scams appear as job offers. The victim is promised payment for completing cryptocurrency-related tasks. Once compensation is agreed upon, they are informed that an additional fee or taxes must be paid upfront to receive the money. For example, if the agreed compensation is €10,000, the "employee" is required to pay 20% in taxes first. Enticed by the prospect of substantial earnings, the victim transfers the requested sum, only to find that they neither receive the promised payment nor recover the upfront fee. The amounts lost in such scams typically range from €2,000 to €3,000, but reports have also been received of much larger losses.

SCAMS IMPERSONATING BANKS AND POSTAL SERVICE PROVIDERS CONTINUED

Once again, numerous reports were received about phishing emails and SMS messages sent in the name of postal service providers or banks. This type of fraud has been popular for years and shows no signs of abating. Broadly speaking, these phishing scams fall into two categories.

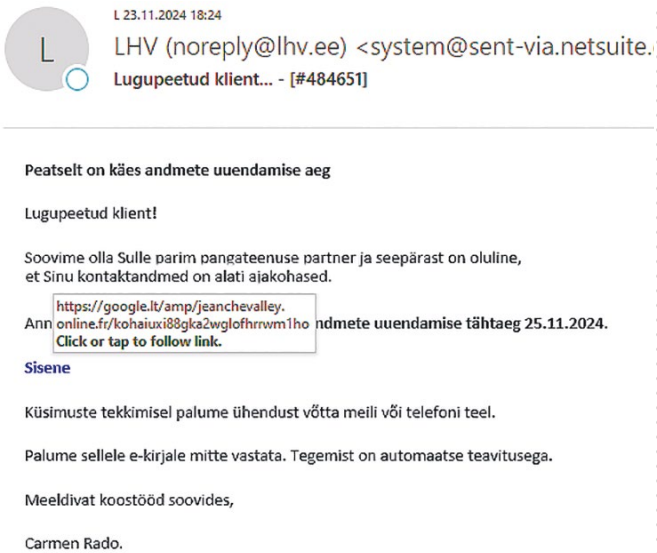
1. The first involves emails or SMS messages sent in the name of service providers such as Omniva, DPD or DHL, claiming that a parcel cannot be delivered due to an incorrect address, unpaid delivery fees or customs charges. Often,



Police caught the creator of phishing kits

On 5 June, Estonian National Criminal Police charged a 22-year-old man suspected of developing phishing kits and selling them on the Telegram app. These kits enabled users to create phishing websites and collect people's login credentials. With these tools, it was possible to bypass two-factor authentication systems used by platforms such as Microsoft 365, PayPal, Google, Dropbox and Binance.

This case highlights the growing trend of cybercrime becoming more service-based, where the person conducting the attacks and the one providing the tools are often different individuals. Fraudsters who create such services are also of interest to the police, as cybercriminals are increasingly becoming a key link in the world of international organised crime. It is crucial to disrupt this chain at an early stage.


L 23.11.2024 18:24

LHV (noreply@lhv.ee) <system@sent-via.netsuite.

Lugupeetud klient... - [#484651]

Peatselt on käes andmete uuendamise aeg

Lugupeetud klient!

Soovime olla Sulle parim pangateenuse partner ja seepärast on oluline, et Sinu kontaktandmed on alati ajakohased.

Ann https://google.lt/amp/jeanchevalley.online.fr/kohaiuxi88gka2wglofhrrwm1ho Click or tap to follow link. ndmete uuendamise tähtaeg 25.11.2024.

Sisene

Küsimuste tekkimisel palume ühendust võtta meili või telefoni teel.

Palume sellele e-kirjale mitte vastata. Tegemist on automaatse teavitusega.

Meeldivat koostööd soovides,

Carmen Rado.

these messages ask for a small payment, typically a few euros, for customs or postal services. However, once users enter their payment card details, significantly larger sums are withdrawn from their accounts. Losses from such scams typically range from a few hundred to tens of thousands of euros.

2. The second type involves emails purportedly sent by a popular bank, asking recipients to update their information. The sender's address is arbitrary, and the email contains a suspicious link that does not belong to the claimed bank. These emails often stress urgency and set a deadline for completing the task. Unfortunately, many people overlook these warning signs and proceed to update their details. The user is directed to a fake website, where they are prompted to log in using the Smart-ID authentication service and enter their PIN codes.

In both cases, users can be almost certain they will not recover their money. The most important step is to carefully check the link included in the email or message to make sure the domain is legitimate. Suspicious addresses usually reveal that the message is not authentic. Banks never send emails with links for updating information; they only request updates via their official apps or websites. Similarly, Omniva and other postal service providers never ask users to enter their details on external websites.

Four examples of successful scams

1. In August, Kalle (all names have been changed) received a message from Omniva claiming that his parcel had been returned due to an incorrect address and asking him to update the delivery address. On the phishing site, he was asked to select the correct parcel locker and pay €4. Kalle entered his card details and noticed that the page kept loading, but he didn't give it much thought. The next morning, however, he discovered that over €1,300 had been withdrawn from his account. Although he cancelled his bank card, the lost money could not be recovered.

2. In September, Malle was selling a refrigerator on Facebook Marketplace. The buyer claimed they could not pick up the item themselves and suggested using Cargobus courier services instead. Malle was sent a link and redirected to a fake Cargobus page to make a payment confirming the refrigerator's transport. Trusting the process, she entered her card details, only to find that €3,900 had disappeared from her account moments later. The payment could not be reversed, and the scammer succeeded.

3. In October, Helle received an email that appeared to be from LHV Bank, asking her to update her details. She entered her banking information on the page opened via the link and later discovered that €950 had been withdrawn from her account. She tried calling and emailing the bank, but as it was outside working hours, she could only reach them the following morning. Unfortunately, it was too late to recover the money.

4. Ülle booked an accommodation on Booking.com. She carefully reviewed other visitors' ratings, photos of the property and the price: the offer seemed both attractive and credible. The site featured dozens of photos of the property and several positive reviews from users. Although payments should typically be made through Booking.com, the host sent Ülle separate bank account details for payment. After receiving her transfer, the host disappeared without a trace, and the property was removed from the portal.

RANSOMWARE VICTIMS: schools and businesses

Although Estonia once again avoided society-wide ransomware attacks last year, some businesses, schools and a dental clinic found their systems infiltrated and their data locked.

A ransomware attack is one of the most distressing forms of cyberattack as it can halt an organisation's operations and jeopardise personal data. While the global number of ransomware attacks and the associated damages increased in 2024, the data available to us suggests a different trend in Estonia. CERT-EE registered around 10 ransomware incidents, fewer than in previous years. However, it is important to note that many victims do not report such incidents.

TWO SCHOOLS, TWO DIFFERENT OUTCOMES

In 2024, two Estonian schools fell victim to ransomware attacks. At the beginning of June, during the busy exam period, Tallinn Health Care College had to manage the aftermath of an attack. The attacker encrypted approximately 1.5 terabytes of data on the school's server, including files belonging to more than 200 staff members and students. Fortunately, the school had a recent backup, enabling them to restore the files and services by the next day.

Two weeks before the start of the new school year, on 16 August, staff at Järvamaa Vocational Training Centre discovered that all data on the school's servers had been encrypted. This attack caused more significant damage, as there was no backup of the data.

ATTACKS THAT HALTED BUSINESS OPERATIONS

At the end of July, a ransomware attack hit a small company in Tartu, and the attackers encrypted files on four computers. The attack disrupted the company's regular operations.

About a week later, ransomware halted operations at a retail company in southern Estonia. Attackers gained access to the backup server, preventing the company from restoring its data.

On 1 November, a dental clinic fell victim to a ransomware attack that resulted in its data being encrypted. Since there was no functional backup, the clinic was unable to recover its files.

WHY DO SUCH ATTACKS HAPPEN?

An analysis of ransomware attacks that occurred in 2024 highlights vulnerabilities related to Remote Desktop Protocol (RDP) applications and network devices.

In nearly one-third of cases, attackers gained access to systems through Remote Desktop applications that were protected by weak passwords



What to do if you have fallen victim to a ransomware attack

- Disconnect the infected device from the network (don't forget to disable wireless connections).
- Notify CERT-EE (cert@cert.ee) for guidance on resolving the incident and advice on preventing similar attacks in the future.
- If infected, restore the operating system from a backup or reinstall it to avoid reinfection. Before restoring from a backup, ensure that it is free of malware. Carefully consider the risks before contacting the attackers.
- Paying the ransom offers no guarantee that your files will be decrypted or that stolen data will not be published. Instead, paying will signal to the attackers that their actions were successful, which may make you a target for future attacks.

and lacked additional security measures such as VPNs, two-factor authentication, IP-based restrictions, logging and monitoring. In light of these incidents, we recommend RDP users review the threat assessment available on RIA's website (ria.ee/media/929/download), which outlines the risks associated with the Remote Desktop Protocol and how to mitigate them.

Several organisations also became victims of ransomware attacks in 2024 due to outdated network devices, unpatched software or insecurely configured management interfaces. In one case, a network device's management interface was publicly accessible on the internet, and the default administrator password was still used, while the server's software was not up to date. In another instance, a router with a long-known vulnerability was in use, despite the device manufacturer having stopped releasing security updates back in 2022. In such cases, purchasing a new device is essential. Delays in replacing outdated equipment can lead to extremely costly consequences.

UNIDENTIFIED INFECTION METHODS

In several instances, the exact method by which ransomware entered the system remained unknown. This uncertainty often stems from a lack of logging. While attackers sometimes delete logs to cover their tracks, in many cases, they do not need to, as the systems simply do not have logs. Without knowledge of how attackers accessed the system, organisations face a significant risk of intruders exploiting the same entry point again.

In nearly one-third of cases, attackers gained access to systems through Remote Desktop applications that were protected by weak passwords and lacked additional security measures.

Record number of VULNERABILITIES

Last year, over 40,000 security vulnerabilities were reported. These affected popular content management systems, network devices, and e-commerce platforms, among others. Much to the advantage of attackers, users of vulnerable software were often slow to update it.

The second week of August started with an alarming incident at the Estonian Transport Administration. After a security system flagged suspicious activity on the organisation's network, a closer investigation soon revealed an unpleasant truth: an attacker had compromised the system used to manage the agency's computers and devices and gained administrator-level access. Although initial concerns arose that data might have been stolen, a subsequent investigation ruled this out.

The solution used for the agency's remote device management was Fortinet's FortiClient EMS. This software had a critical vulnerability (CVE-2023-48788), disclosed by Fortinet on 12 March, along with a new version addressing the issue. Unfortunately, the Transport Administration had not installed this essential update. Attackers found the vulnerable system, exploited the weakness, and breached the network.

How to protect yourself against the exploitation of vulnerabilities

- Keep the operating systems, firmware, applications and other software on all your systems up to date.
- Replace outdated devices that are no longer supported with security updates from the manufacturer.
- Protect your network and administrative interfaces. Utilise VPNs and limit access to devices, particularly system management interfaces, to specified IP addresses only.

ONE OF MANY

Unfortunately, there are many such stories involving both public- and private-sector organisations.

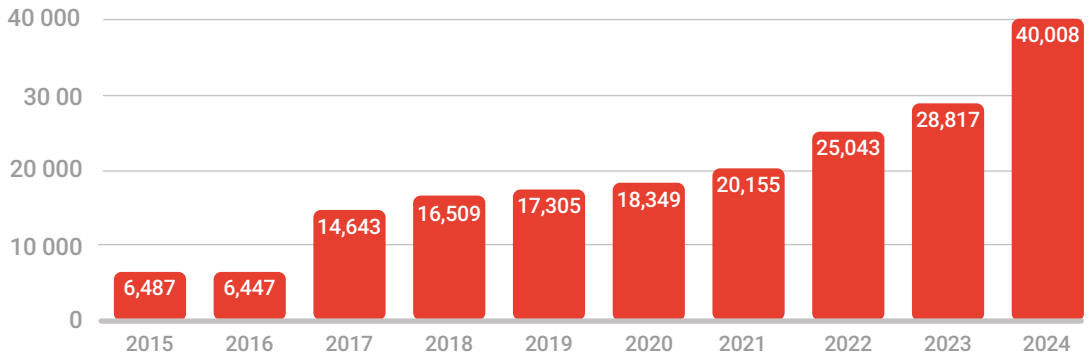
In early February, a government agency reported that its VPN servers had been compromised. The attack, which began in January, exploited vulnerabilities in Ivanti software that had been publicly disclosed just 12 days earlier.

In August, CERT-EE alerted the administrator of an online store about a critical vulnerability in their Magento platform. Unfortunately, the store owner did not act on the warning, and in November, the online store was compromised using that same vulnerability.

CERT-EE actively scans Estonia's cyberspace for systems with critical vulnerabilities. When such websites or devices are identified, their owners are notified and advised on how to fix the issues.

In 2023, CERT-EE issued 2,427 notifications; last year, this number more than tripled to 7,955. Of these, the largest share – 2,462 – were warnings about vulnerabilities in WordPress and its plugins, while 263 related to vulnerabilities in

Number of reported vulnerabilities 2015–2024



Source: nvd.nist.gov

Magento. Hundreds of notifications were also sent to owners of network devices and management systems with critical vulnerabilities.

EXPLOITING A ZERO-DAY VULNERABILITY IN ESTONIA

On 23 October, information about a zero-day vulnerability in FortiManager (CVE-2024-47575) was made public. This vulnerability in a critical FortiManager function allowed attackers to execute arbitrary commands within the system due to the absence of authentication. Fortinet had warned its clients about the potential vulnerability a few days earlier, advising them to update the software and implement additional protective measures. However, in Estonia, this vulnerability was already exploited on 22 October, with attackers gaining control of two servers belonging to one organisation.

GLOBAL TRENDS

In 2024, the number of reported vulnerabilities grew significantly. The number of reported vulnerabilities surged in 2024, reaching 40,008 globally – a one-third increase from the 28,817 identified in 2023.

Global trends included the exploitation of zero-day vulnerabilities in the firmware of network devices and network management systems. For example, two zero-day vulnerabilities in Ivanti software (CVE-2023-46805 and CVE-2024-21887) were exploited by groups linked to China. These vulnerabilities allowed attackers to bypass authentication and inject commands.

CERT-EE discovered a critical vulnerability in Palo Alto software

CERT-EE identified and documented a critical vulnerability (CVE-2024-3393) in devices running Palo Alto Networks' operating system, PAN-OS. The vulnerability allowed attackers to send a specially designed malicious network packet that caused the firewall to freeze, rendering it unusable in a denial-of-service state. When in a denial-of-service state, the firewall halts all network traffic, which disrupts internet connectivity and disables online services reliant on the network. Working in collaboration, CERT-EE and Palo Alto engineers identified the root cause of the issue, and Palo Alto released an updated version of PAN-OS to address the vulnerability.

Cybercriminals also continued to target devices with older, known vulnerabilities, often exploiting them for ransomware attacks or adding them to botnets.

As in previous years, numerous critical vulnerabilities were discovered in web content management systems and e-commerce software.

The prevalence of zero-day vulnerabilities and the ongoing exploitation of older vulnerabilities highlight the need for a systematic approach to this issue. Organisations must establish and follow vulnerability management processes and bolster their network security with additional protective measures.

2024: Events in international cyberspace

The year 2024 saw influence operations surrounding elections, breaches by Chinese hackers in telecom companies, and widespread IT system disruptions caused by CrowdStrike.

It was also an extraordinary year for elections. In addition to the US presidential election, the UK general election, and the European Parliament election, general or local elections were held in nearly 100 countries worldwide in 2024. For many nations, this meant increased pressure in cyberspace, with attacks ranging from denial-of-service (DoS) and defacement attempts on political party websites to information operations designed to shape voter preferences.

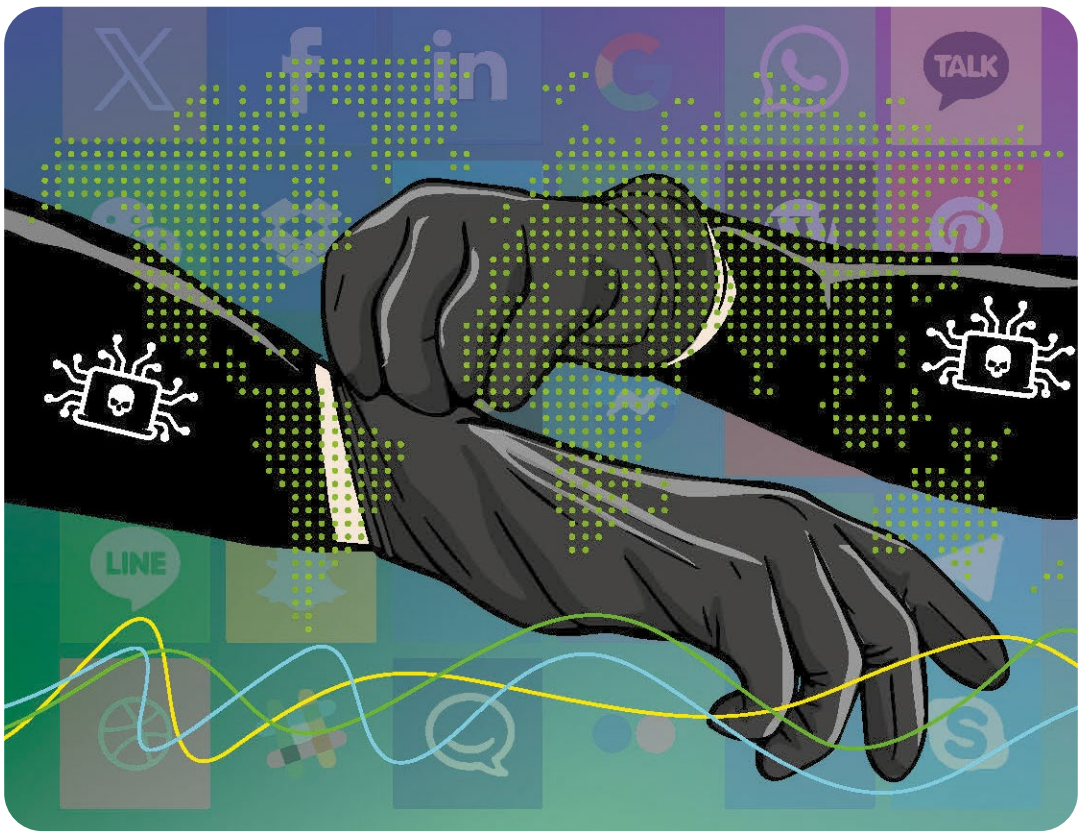
PRESIDENTIAL ELECTION FIRST ROUND ANNULLED IN ROMANIA

An information operation in the context of elections generally involves the coordinated dissemination and amplification of fake news or half-truths on social media, aiming to gain votes for a particular candidate or, conversely, to diminish the support of their opponent. When foreign states conduct such operations, the situation becomes particularly grave, as it amounts to external interference in a country's democratic process.

The most drastic example this year came from Romania, where the Constitutional Court decided to annul the results of the first round of presidential elections held in November. According to the country's intelligence services, Russia had organised a coordinated influence campaign on TikTok in support of a far-right candidate. The intelligence services also reported that over 85,000 cyberattacks were carried out against election infrastructure with various objectives, such as gaining access, altering election-related information or disrupting its availability.

SALT TYPHOON TARGETS TELECOM COMPANIES

Iran, China and Russia also attempted to influence the US presidential election. In the final months of the year, reports began to emerge about Chinese state-backed hackers successfully infiltrating the infrastructure of several major



American telecom companies, including AT&T, T-Mobile, and Verizon. The group responsible was Salt Typhoon, and the incident is believed to be the most extensive cyberespionage campaign targeting the Western telecommunications sector to date.

According to the White House, Chinese hackers had been embedded in telecom companies for one or two years, affecting not only the US but also several European and Southeast Asian countries. Salt Typhoon's activities first gained media attention after reports surfaced that they had targeted the phone data of several high-ranking US politicians, including the vice president and president.

Alongside state-sponsored espionage groups, cybercriminals also targeted the telecom sector. In October, Free, the second-largest internet service provider in France, suffered a breach in which a database containing the details of 19 million customer accounts was stolen and offered for sale on the dark web.

The US telecom company AT&T was also affected in the spring by the compromise of Snowflake's data warehouse, which was among the largest service provider-based attacks of the year. Snowflake, a cloud-based platform for storing and analysing large volumes of data, became a target when the hacker group Shiny-Hunters found some Snowflake user credentials for sale on the dark web. Seizing the opportunity, they used the credentials to attempt

Chinese hackers had been embedded in telecom companies for one or two years, affecting not only the US but also several European and Southeast Asian countries.

access to sensitive data belonging to Snowflake's high-profile clients. The Snowflake data breach affected at least nine major corporations and millions of their customers. Among the victims was Ticketmaster, whose leaked data caused significant disruption, including chaos around already scarce tickets for a Taylor Swift concert tour.

CROWDSTRIKE SOFTWARE GLITCH DISRUPTED MILLIONS OF COMPUTERS

While high-impact cyber incidents are usually associated with malicious attacks and prevented by cybersecurity companies through their protective solutions, one of the most significant IT incidents in history was caused by a colossal blunder by the renowned cybersecurity provider CrowdStrike.

Last summer, the company released a faulty update for one of its flagship products, the CrowdStrike Falcon platform, which on 19 July caused millions of Windows systems to stop functioning. The fallout included flight cancellations across the US and Europe, disruptions to rail services in the UK, interruptions at a Finnish news agency, and the closure of shopping centres in Australia, to name just a few examples of the widespread global disruptions. Estonia was also affected: some computers at grid operator Elektrilevi were down for a few hours, and check-in for Ryanair flights at Tallinn Airport had to be carried out manually.

CrowdStrike's global IT disruption

In the early hours of 19 July, at 4:24 am, CrowdStrike released a routine security update for the sensor in its cloud-based CrowdStrike Falcon antivirus system.

But the update turned out to be flawed. The automatically updated sensor affected the underlying settings of many Windows systems, causing them to stop functioning. It is estimated that the operation of at least 8.5 million devices was disrupted globally.

This led to disruptions and closures across aviation, finance, healthcare, commerce and media sectors worldwide, with global damages estimated in the billions of dollars.

CrowdStrike quickly identified the error and issued a corrected update at 5:27 am the same morning. However, already affected devices had to be restored manually, which meant that the interruptions lasted anywhere from hours to days or even weeks, depending on the sector and organisation.

ATTACKS ON THE HEALTHCARE SECTOR

Cyberattackers often target critical services, and as in previous years, several serious incidents were linked to the healthcare sector. In many cases, attackers bypassed the healthcare institutions themselves and targeted these institutions' critical service providers instead.
In February, the ransomware group BlackCat attacked the US company Change Healthcare, which connects patients, doctors and insurance providers. As a result, healthcare billing and patient reimbursements across the country were disrupted, with healthcare institutions reportedly suffering losses amounting to tens of millions of dollars. The attack also led to the theft of sensitive data on 100 million Americans – about one in three people – followed by additional ransom demands months later.

In Romania, a February ransomware attack on the medical sector's information system forced around 100 hospitals to go offline and temporarily resort to handwritten prescriptions and patient records. In early June, a ransomware attack hit Synnovis, a pathology and diagnostic service provider collaborating with several major hospitals in London. This led to several days during which rapid blood tests and transfusions could not be performed, resulting in postponed surgeries and cancelled appointments.

DATA LEAK FROM HELSINKI CITY GOVERNMENT

Data breaches have become increasingly common in today's digitalised society, but 2024 saw some particularly notable cases. Early May brought bad news for Finland, as it was revealed that the education department of the Helsinki City Government had suffered a cyberattack resulting in the theft of data belonging to up to

150,000 individuals, including children and young people's personal details and health information.

The attack exploited a server running outdated software, which had been slated for replacement but was delayed due to a busy maintenance schedule. Given that serious data breaches have shaken Finnish society before, the government decided to involve the Safety Investigation Authority, which is responsible for investigating and preventing major incidents.

During the first week of May, it was also revealed that over 225,000 personal records of active-duty personnel, veterans and reservists in the United Kingdom armed forces were leaked through payroll system used by the UK Ministry of Defence. The leaked data included names and bank account information – sensitive details likely to be of interest to hostile intelligence services.

The breach was reportedly made possible due to the service provider's inadequate cybersecurity standards. This underlined an issue that many countries, including Estonia, continue to grapple with: how to mitigate cyber risks in critical sectors that rely on external service providers.

$25 MILLION LOST DUE TO DEEPFAKE TECHNOLOGY

Last year, we predicted that rapidly advancing artificial intelligence would transform the cyber landscape. In 2024, phishing emails and messages, enhanced by large language models, became more realistic and accurate, even in less widely spoken languages. However, the most alarming developments were tied to deepfake technology in both voice and video.

In February, Hong Kong police investigated a case where a finance officer at a multinational corporation participated in a video call with colleagues and later transferred $25 million from the company account, acting on what appeared to be instructions from the CFO during the call. The entire video call turned out to be fake – the 'colleagues' on-screen were deepfake creations, made to look and sound exactly like their real counterparts.

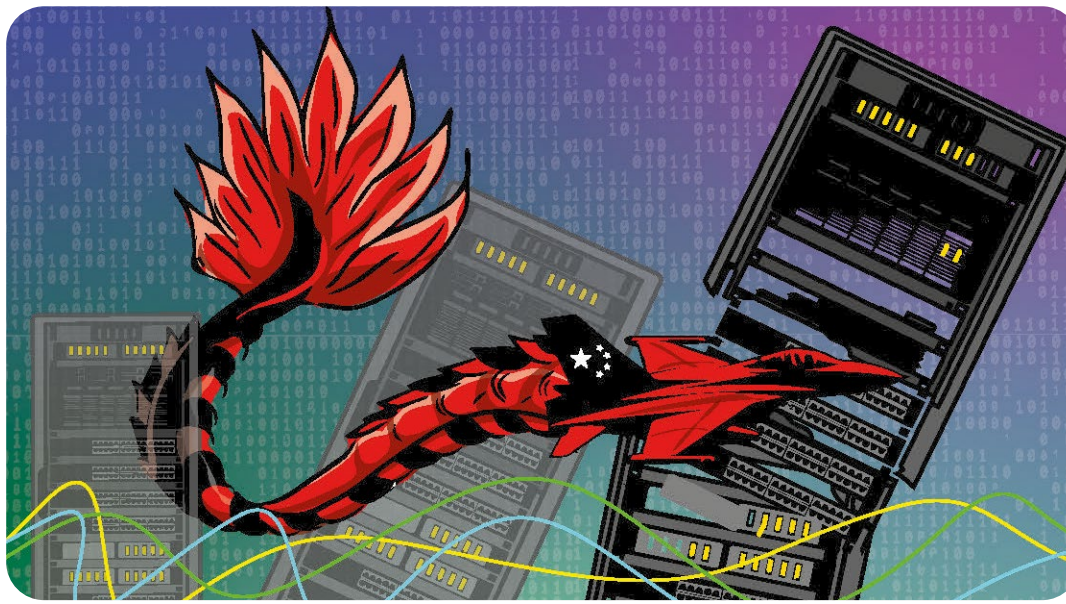
While creating fake videos requires some effort and time, synthesising a specific individual's voice can take just 10 minutes using widely available software. In one case in the US, for example, a mother received a call from a stranger claiming her daughter had caused a car accident and demanded compensation. To lend credibility to the story, the phone was passed to the 'daughter', who sounded distressed, admitted fault and urged her mother to comply. In reality, the daughter's voice had been faked.

While creating fake videos requires some effort and time, synthesising a specific individual's voice can take just 10 minutes using widely available software.

Scammers often use public speech samples, such as TikTok videos or conference recordings, to create a fake voice. In this case, however, the daughter had received several strange phone calls in the days leading up to the scam, which she did not think to hang up immediately. The family believes these calls were used to train the AI tool to replicate her voice and mannerisms.

GROWING COLLABORATION AMONG HACKTIVISTS

In recent years, hacktivists have made their presence felt in cyberspace, in Estonia, and globally, attempting to disrupt the daily lives of nations they view as adversaries through cyberattacks. In 2024, they continued their efforts, targeting high-profile events such as the Paris Olympics and the UEFA European Championship. These attacks primarily involved basic denial-of-service (DoS) attacks on government websites, which were largely ineffective. However, there are signs that cooperation among various hacktivist groups is gradually growing, enabling them to occasionally expand their activities geographically. For example, pro-Kremlin hacktivists added South Korea to their list of targets after the country condemned North Korean soldiers' involvement in Russia's war in Ukraine.



THE RED DRAGON spreads its wings

China's ambition to become the world's leading power by 2050 is backed by its state-sponsored cyber groups. Cyber threats linked to China generally fall into three categories: cyberattacks, technological dependence and data transfers to China.

Chinese-affiliated groups are arguably the most capable and sophisticated anti-Western forces conducting cyber operations. For example, US Senator Mark Warner has remarked that compared to Chinese activities, Russian operations seem like child's play. Unlike Russia, China often operates more covertly, focusing on cyber espionage and pre-positioning rather than service disruptions. While there are many Chinese-linked cyber groups, three distinct 'typhoons' stand out.

RIDING THE TYPHOON WAVES

In the autumn of 2024, US authorities reported that the Chinese-affiliated group Salt Typhoon had infiltrated American telecommunications networks. This access enabled the group to obtain call logs and unencrypted text messages

and even monitor conversations involving former President Donald Trump and presidential candidate Kamala Harris's teams.

Another actor, Flax Typhoon, has taken control of hundreds of thousands of devices globally, forming an army of so-called zombie devices, also known as a botnet.

Meanwhile, Volt Typhoon has embedded itself within critical infrastructure in the United States. According to the White House, Volt Typhoon's objective is less about stealing data and more about preparing to disrupt essential services – such as water, communications and heating – should China ever deem it necessary.

'MADE IN CHINA'

Chances are, your phone was made in China. The same likely applies to your robot vacuum cleaner, air fryer and many other items in your home or office. It's harder to find products not made in China than those that are. While Chinese goods may often appear cheaper and beneficial to consumers, the reality is more complex. The lower prices are not only due to cheaper labour but also to substantial state support for Chinese industries. This dynamic can lead to a situation where companies outside China struggle to compete, which might eventually make our critical products and services dependent on Chinese suppliers.

For example, Estonia's electricity network operator, Elering, highlighted in its energy security report that a significant proportion of solar energy installations in Estonia rely on inverters produced by a single Chinese manufacturer. This dependency poses considerable risks to supply security, including vulnerabilities to cyberattacks, data monitoring by the Chinese government, and reliance on a single supplier for maintenance and procurement.

TIKTOK IS WATCHING YOU

It is widely known that TikTok collects user data, but is that a problem? Many might argue, 'I have nothing to hide!' However, personal data is a valuable asset and should be handled responsibly, which is precisely what the European Union's General Data Protection Regulation (GDPR) aims to enforce. Chinese laws, however, are different. Under Chinese law, all companies are required to share their data with the state – a fact publicly confirmed by TikTok's CEO in court. Beyond knowing your favourite cat or dance videos, TikTok collects data about your device, contacts, calendar, other apps, Wi-Fi connections and more. All of this information is also used to develop artificial intelligence in China.

And remember your internet-connected air fryer? If it's made in China, it's likely sending data there as well.

China is one of the world's most powerful nations and has openly challenged democratic countries, seeking to expand its influence in the digital realm as well as other spheres. Through various means, it aims to assert its dominance in cyberspace. The Estonian Information System Authority advises businesses and other organisations to carefully evaluate the reliability of their supply chains; individuals should reconsider which apps and products they use.

Three attacks suspected to involve Chinese groups

Salt Typhoon's hacking operation began in the spring of 2024 and continues to this day. Public reports indicate that the group infiltrated the networks of at least 80 telecommunications companies worldwide, making this one of the most severe cyberattacks in history. The attackers allegedly managed to breach Donald Trump's phone, gaining access to unencrypted communications, such as SMS messages and other data. The full extent of the damage is still under investigation.

Flax Typhoon infected over 200,000 devices, including routers and surveillance cameras, and formed a botnet used to conduct cyberattacks.

Hackers infiltrated the **UK Ministry of Defence**, stealing the personal data of more than 270,000 current and former military personnel. The stolen information included first and last names, bank details, addresses, and other personal records. The attack is suspected to be the work of Chinese-affiliated actors.

CYBER-SECURITY is a matter of national sustainability

Cybersecurity is more than an IT concern – it is a matter of national sustainability, argue Taavi Viilukas, Irina Klementi and Kaido Tee from the National Cybersecurity Department of the Ministry of Justice and Digital Affairs.

The digital nervous system that underpins public- and private-sector services is highly complex. The reliability of each node depends on the presence and integrity of others. If one node becomes inaccessible, it disrupts all interconnected systems and services. This interdependence makes cybersecurity an integral part of the broader framework, which requires constant attention.

DIRECTION AND PURPOSE

Without a national policy and strategic direction in cybersecurity, efforts would resemble Brownian motion – random, uncoordinated movements lacking a unified goal. Imagine a country where cybersecurity is managed through isolated projects and ad hoc decisions. Each organisation would act according to its best judgment, but the result would be a fragmented system unable to respond effectively to threats or ensure the continuity of critical services. Such a state would undoubtedly be highly vulnerable.

It is, therefore, essential for digitally advanced nations, including Estonia, to establish and implement cybersecurity policies grounded in a long-term vision and a systematic approach. Citizens, businesses, critical infrastructure and the public sector must understand and commit to a shared goal. Unified policies ensure that cybersecurity measures are coordinated, mutually reinforcing and quickly adaptable to evolving threats. Only then can a country maintain resilience and security.

The architecture of national information systems must account for potential interdependencies and risks. Every new system or technology should be assessed for its impact on the broader ecosystem, guided by thorough risk analysis. Risk assessment is not a one-time project but an ongoing process that adapts to changing threat landscapes and technological developments.

Cybersecurity is more than an IT concern; it is a matter of national sustainability. Just as system resilience testing and regular risk assess-



Photo: JMinistry of Justice and Digital Affairs

Kaido Tee, Irina Klementi and Taavi Viilukas.

ments are vital, so too is analysing the overall resilience of organisations and the state as a whole.

A UNIFIED LEGAL FRAMEWORK

Given the evolving security landscape, it is essential to harmonise the legal framework for cybersecurity, network and information security, and crisis management to make sure it reflects best practices and secures the continuity and safety of Estonia's services in even the most challenging situations.

In the near future, it will be important to incorporate international directives into Estonian law in a way that balances national defence, business freedom and cybersecurity requirements.

European Union (EU) directives form a critical part of Estonia's cybersecurity framework. However, their implementation should avoid rigid and unconsidered solutions. Too often, Estonian legislators fall into the trap of rigorously and meticulously implementing EU directives and regulations while losing sight of their purpose and intended benefits. A smart approach to implementing EU directives involves analysing their impact and adapting them to local conditions.

For example, when adopting the NIS2 directive in Estonia – which outlines cybersecurity requirements for essential service providers – the focus should go beyond merely meeting technical requirements. Instead, priority should be given to fostering local business development and strengthening the country's digital resilience. This involves considering the size of local businesses, the unique characteristics of various sectors and the state of infrastructure development. Such an approach ensures that regulations genuinely enhance security rather than devolving into burdensome bureaucracy. Otherwise, large international corporations with greater resources and experience would gain a competitive edge – an outcome that is clearly not in Estonia's best interests.

LOOKING TO THE FUTURE

As policymakers shaping cybersecurity, we must address immediate issues while also preparing for the future. Within the next decade, quantum computing will fundamentally transform data protection and cybersecurity, breaking the currently secure and reliable cryptographic methods. Thus, it is essential to begin adopting quantum-resistant algorithms, also known as post-quantum cryptography.

> Within the next decade, quantum computing will fundamentally transform data protection and cybersecurity.

Cybersecurity requires more than implementing physical, technical and procedural measures. It demands a systemic and community-based approach to protecting the nation as a whole. Cybersecurity is a matter of national sustainability and must not be underestimated. To enhance our defences, we must combine our knowledge and skills and collaborate not only within the public sector but also with the private sector and internationally. Cybersecurity demands a unified 'we' mindset, moving beyond blame games and divisive 'us versus them' attitudes to work together towards a shared goal. Only then can we ensure the security of our digital state.

ESTONIAN SCHOOLS should prioritise cybersecurity

In Estonia, cybersecurity requirements apply to nearly 1,000 educational institutions, ranging from local government-run kindergartens and schools to large public universities. However, the level of cybersecurity measures in schools varies widely, and the overall situation leaves much to be desired.

The Estonian Information System Authority (RIA) registers dozens of cyber incidents affecting educational institutions each year, most of which could be prevented with minimal effort. Schools face data breaches, account and website hijackings, scams, denial-of-service and ransomware attacks, and many other threats. Let us explore the most common risks and recommendations for avoiding them.

DATA BREACHES AFFECTING STUDENTS AND STAFF

Over the past few years, three cases in Estonia have involved the leakage of personal data from students and school staff, with at least one instance where the stolen data was put up for sale. These cases primarily involved contact and account information, which, while serious, are not the most sensitive types of data.

However, schools may also handle highly sensitive information, such as students' health-related data. For example, development plans for children with special educational needs may include details of behavioural issues, health problems or even interactions with the police. If such information becomes public, it can severely damage a child's future prospects.

School healthcare workers also handle students' health data, which is another potential vulnerability. One significant risk arises when a school nurse's computer is connected to the same network as the rest of the school community (and anyone else with the password). To improve security, schools should segment their networks by creating separate sub-networks for different groups, such as teachers, students, administrative staff and medical personnel. Although this is not a particularly complex task, it is often overlooked due to a lack of awareness.

Poorly secured school networks have even been exploited for criminal activities, including drug trafficking, leading to police involvement with affected schools. Cyber incidents jeopardise not only personal data but also the reputation of school staff and institutions. Repeated



incidents, such as account hijackings that result in inappropriate mass emails or phishing attempts being sent to students, parents or colleagues, can cause lasting reputational damage.

Such incidents can usually be avoided by vigilance and adherence to basic cybersecurity hygiene. Account takeovers often begin with phishing links, malware attachments, unpatched software, carelessly discarded papers with passwords, or a teacher leaving their computer unlocked and unattended – an easy temptation for a mischievous student. Enabling multi-factor authentication is strongly recommended to protect user accounts better.

The loss of teaching materials due to technical errors or cyberattacks can impose a heavy burden on teachers, requiring hours of additional work to recreate the lost content.

YEARS OF WORK CAN BE ERASED IN MOMENTS

Many cyber incidents stem from technical failures rather than malicious intent. Today, a significant proportion of teaching materials are created digitally, and learning outcomes are often recorded exclusively in digital formats. The loss of teaching materials due to technical errors or cyberattacks can impose a heavy burden on teachers, requiring hours of additional work to recreate the lost content. Years of work can disappear in an instant. Similarly, the deletion or malicious alteration of grades can cause significant confusion for students and future complications when verifying academic records.

In August 2024, all server data at the Järvamaa Vocational Training Centre was lost in a ransomware attack, with no backups available. The Tallinn Health Care College was more fortunate in June, as it managed to restore staff

→

and student files the following day using backups. These cases highlight the critical importance of data backups, which should always be stored separately from other systems.

Estonian schools also frequently experience denial-of-service attacks, which can temporarily disrupt internet access and daily operations. Analysis of attack patterns suggests that many of these incidents are likely orchestrated by students. Such attacks are relatively simple to execute and can even be purchased as a service from cybercriminals. However, school information systems should be designed to withstand these types of large-scale intrusions.

> Implementing cybersecurity requirements may initially seem daunting for school leaders, but a step-by-step approach and a clear plan can make it manageable.

Although it is impossible to eliminate all risks, every incident provides an opportunity to learn. Those responsible for information security in schools should share their experiences with peers to support collective learning and help prevent similar incidents elsewhere. Unfortunately, these stories are often kept quiet. The absence of open discussion within the community reduces awareness and perpetuates the mistaken belief that such incidents are uncommon. As the saying goes, a wise person learns from others' mistakes, while a fool learns only from their own.

SCHOOL LEADERS SHOULD SEEK GUIDANCE FROM STAKEHOLDERS

Cybersecurity in schools is not always within their direct control. Last year, for example, there were recurring issues with the examination information system and the Moodle learning environment, both managed by the Ministry of Education and Research. These incidents underline the importance of investing in centralised e-services.

Estonian schools also rely on various platforms and services, such as electronic school management systems, provided by private companies, which often have little or no competition, leaving schools with no viable alternatives. Legally, however, educational institutions are responsible for ensuring data protection when outsourcing such services. This can be achieved through informed and well-considered procurement processes, with assistance available through RIA's online training programme. Schools would benefit from pooling their resources and collectively discussing their needs to strengthen their position when negotiating with service providers. The experience of the Estonian Society of Family Doctors shows

Recommendations for schools starting with cybersecurity

1. Raise cybersecurity awareness. Many cyber threats can be prevented by raising staff awareness. We recommend starting with RIA's free Cyber Test , which around 100 schools across Estonia have already adopted.
2. Discuss with the school's owner. School leaders should address information security with the institution's owner, considering resource allocation and organisational structure. For example, they could explore organising cybersecurity centrally across all local government institutions, hiring an external service provider or similar solutions.
3. Use RIA's dedicated tool. RIA has developed the E-ITS profile, based on the Estonian Information Security Standard, which focuses on key security requirements for educational institutions. However, each school should further customise the profile to address the institution's unique needs and characteristics.
4. Leadership recommendations. The profile begins with recommendations for school leaders, who play a critical role in promoting information security. Leaders should appoint

that collaboration can facilitate necessary changes to service contracts.

Implementing cybersecurity requirements may initially seem daunting for school leaders, but a step-by-step approach and a clear plan can make it manageable. RIA experts observe that a school's level of cybersecurity rarely depends on its size but instead on the leadership's attitude. It largely hinges on how seriously they value protecting their community's data and ensuring that modern learning and working tools can be used securely, without fear of cyber threats.

The majority of Estonia's educational institutions are owned and budgeted by local governments, so school leaders should consult their municipal or city governments to improve cybersecurity. Since municipalities often manage numerous subordinate institutions that rely on shared information systems, a centralised approach to cybersecurity may be more efficient. This could involve hiring dedicated staff or outsourcing the necessary services to a specialist provider. Examples of municipalities that have adopted such a model include Pärnu City and Saaremaa Municipality.

RIA regularly organises information days and training sessions to assist schools in meeting cybersecurity requirements, many of which are specifically designed for educational institutions. RIA experts are readily available to offer direct guidance to schools on cybersecurity requirements, and inquiries can be sent to kikk@ria.ee.

RIA to increase oversight of schools

Recently, RIA's supervision department has been paying greater attention to educational institutions, as the high number of cyber incidents suggests schools are not adequately addressing information security. In 2025, inspections are planned for state high schools and public universities, with some municipal schools likely to be included as well.

The goal of these inspections is not to punish but to prevent significant data breaches and disruptions in critical educational systems. To achieve this, RIA identifies security vulnerabilities and deficiencies in meeting cybersecurity requirements and guides institutions in resolving any identified issues within a reasonable timeframe. Schools can also negotiate deadlines for implementing the necessary fixes.

If agreements are not honoured or if an institution refuses to cooperate with oversight efforts, RIA has the authority to impose fines. However, fines have only been issued in rare cases. Beyond addressing specific issues at individual institutions, these oversight activities help RIA gain a clearer understanding of the overall state of cybersecurity in Estonia's education sector. This enables the agency to highlight common challenges, improve prevention efforts, and, if necessary, propose regulatory changes or advocate for additional funding.

a responsible person for implementing technical requirements, either from the institution or externally, such as an information security manager, IT specialist or computer science teacher.

5. Inventory and access review. Effective cybersecurity starts with understanding the school's IT assets. Create an inventory of devices and software, and review system and network access for staff and students. Immediately revoke access for graduates and departing employees.

6. Establish information security procedures. Develop an information security policy outlining how IT devices and systems should be used securely within the school.

7. Review service contracts critically. When outsourcing IT services, carefully examine contracts to ensure clarity on what the service includes and how security incidents will be handled.

8. Take advantage of RIA's online training. School information security officers should complete the three RIA-created E-ITS online training modules available on the Digital State Academy website. Each course takes about an hour to complete, provides an overview of the field and offers practical advice:

- E-ITSi ABC
- E-ITSi rakendamine
- Turvaline väljast tellimine

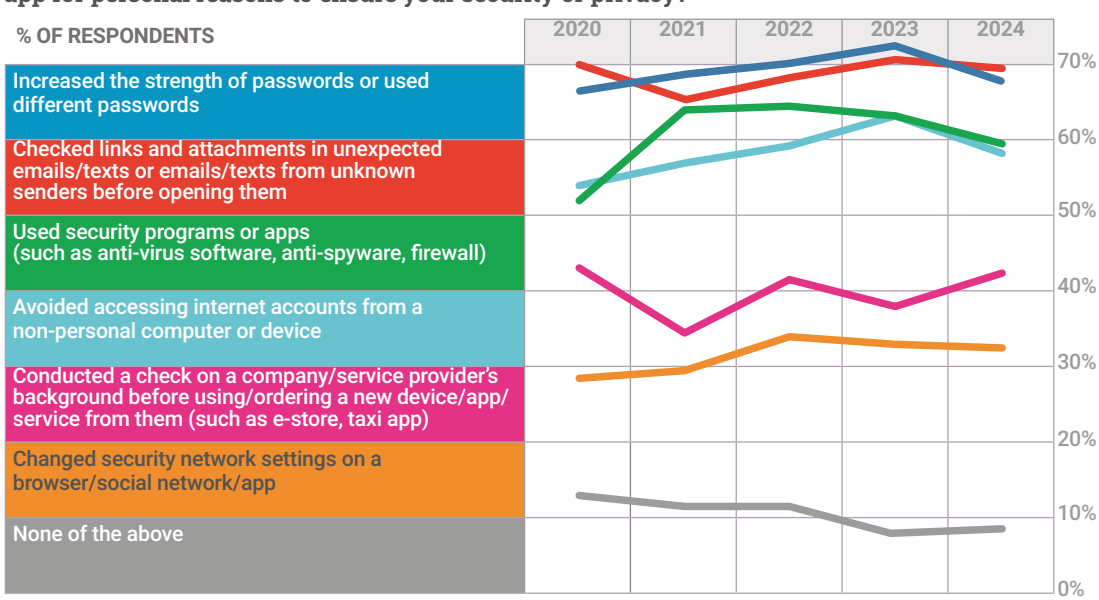
PREVENTION EFFORTS for all generations

In cybersecurity, prevention is always more cost-effective than managing the consequences. With this in mind, we conducted workshops for older adults, launched a campaign aimed at younger generations, and published guides tailored to children and their parents.

Over the years, Estonians' awareness of cyber threats has generally increased. According to Statistics Estonia, fewer than 10% of people have taken no steps to protect themselves online. Nearly three-quarters of internet users carefully scrutinise emails and messages from unknown senders, and a solid 70% follow the advice to use strong, unique passwords across different websites.

Despite this encouraging trend, some concerns remain. While 16–24-year-olds often check the credibility of service providers or

QUESTION: which of these have you done on the internet or an app for personal reasons to ensure your security or privacy?





Some of RIA's cyber security campaign literature.

companies they interact with, their use of other good practices – such as strengthening passwords, adjusting security settings or using antivirus software – has declined.

Previous studies commissioned by the Estonian Information System Authority (RIA) have revealed that many individuals overly trust their critical thinking skills online and believe they are unlikely to become victims of a cyberattack. This overconfidence dulls their sense of risk and leaves them more exposed to threats in the virtual world.

WORKSHOPS FOR OLDER ADULTS AND CAMPAIGNS FOR YOUNGER GENERATIONS

Older adults sometimes struggle to find reliable information online. To address this, RIA partnered with BCS Koolitus to offer face-to-face cybersecurity workshops for middle-aged and older participants. These free workshops taught attendees how to identify online threats and better protect their computers and smart devices. Held in various locations across Estonia, the workshops attracted nearly 500 participants, who found the sessions highly valuable. Many attendees expressed interest in similar short courses to refresh their knowledge and skills in the future.

In October, during International Cybersecurity Month, the focus shifted to younger generations. A public awareness campaign – visible both online and on the streets – encouraged individuals to follow basic cyber hygiene rules and take the time to help their loved ones be more cautious in the digital space.

Cybersecurity Month saw a surge in related content across websites, radio, newspapers and social media. One standout initiative was the TV series 'IT-vaatlik', a collection of short programmes aired on Estonian national television, featuring cybersecurity experts from RIA, the police, the Estonian Banking Association, universities and other organisations. Topics included smart device security, fraud detection and safe remote work practices. The first 15 episodes reached nearly 200,000 viewers. Those who missed the broadcasts can find the episodes on the itvaatlik.ee website, in the ERR archive and on the streaming platform jupiter.err.ee.

GUIDES FOR CHILDREN AND THEIR PARENTS

For the youngest internet users, RIA created interactive guides featuring crosswords and activities that introduce cybersecurity concepts in an engaging and age-appropriate manner. According to Statistics Estonia, nearly half of parents monitor their under-16 children's activities on social media, gaming platforms or other online portals. Similarly, about 50% have applied content restrictions on their child's devices using parental control apps.

Seventy per cent of parents talk to their children about online risks and share advice on safe behaviour. While these conversations are irreplaceable, RIA released guides designed specifically for children and their parents titled 'Safely online' at the start of autumn. These materials are available on the prevention portal itvaatlik.ee. The first 2,000 copies of the children's guides were quickly distributed across Estonia, with more expected soon to help vital knowledge about cyber threats reach even more families.

EU STEPS in cyber security

What did the European Union achieve in cyber security in 2024, and what lies ahead in 2025?

Very few holiday travellers heading to airports in July 2024 could have expected that a cyber incident might suddenly cancel their long-awaited trip. A failed software update from a US cybersecurity provider caused repeated rebooting of computers running the Windows operating system, resulting in billions of euros in damages and disrupting air travel, stock markets, television broadcasts and manufacturing.

The impact of cyber incidents on the general public is set to increase in the coming years, and inaction will not provide relief. What steps is the European Union taking to ensure the continued functioning of individuals, businesses and societies in the golden age of cyberattacks?

The situation with cyberattacks will not improve anytime soon, and we must increasingly consider the unthinkable - this was the observation made in January 2025 by Robert Viola, head of DG CONNECT, the EU's directorate-general responsible for cyber security. His statement, along with the growing number of cyberattack headlines, explains why the EU has adopted numerous cybersecurity regulations in recent years. These regulations aim to enhance the cyber resilience of European citizens, businesses and institutions. Digital solutions have become an essential part of societal functioning, rather than being just a convenient alternative to physical services.

With this in mind, let us review what the EU achieved in cyber security in 2024, and what lies ahead in 2025.

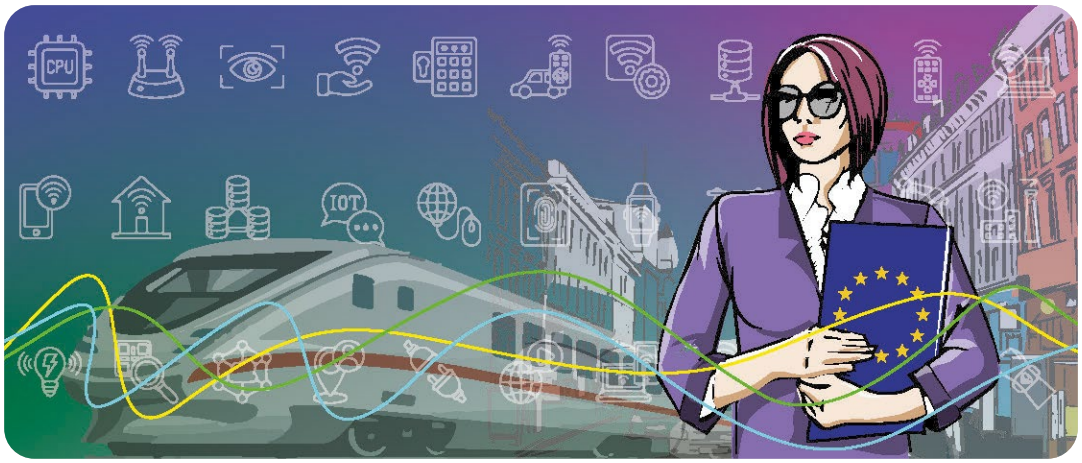
NIS2

In January 2023, the EU's second cybersecurity directive, NIS2, came into effect, with the goal of establishing a consistently high level of cyber security across all member states. Member states had until October 2024 to incorporate it into national law, but Estonia, along with 20 other countries, missed the deadline. According to those drafting the legislation, the process was slowed by continuous refinements to guidelines and sector-specific inquiries. The goal is now to implement NIS2 by mid-2025, at which point the final scope of businesses affected by the directive will become clear. The directive helps essential and important service providers adopt a strategic approach to cyber security, defines how and whom to notify in case of an attack, and sets baseline cybersecurity requirements.

CYBER RESILIENCE ACT

On 10 October 2024, member states adopted the Cyber Resilience Act (CRA), which establishes cybersecurity requirements for digital components and internet-connected devices such as smart TVs and home security cameras. The regulation ensures that products containing digital elements, including Internet of Things (IoT) solutions, remain secure throughout the supply chain and product lifecycle.

The CRA aims to establish uniform cybersecurity requirements for hardware and software products, avoiding regulatory overlap. It applies to products that are directly or indirectly connected to another device or communication



network, excluding those already governed by other EU regulations, such as medical devices, aviation products and vehicles. Products must carry a CE marking, which certifies compliance with the regulation and with safety, health and environmental protection standards. This helps consumers identify secure products and protects both individuals and businesses from insecure digital products.

Unlike NIS2, the CRA has a longer implementation timeline, with a deadline set for December 2027. The European Commission must first establish general standards (Type A) in collaboration with member states, followed by standards for more than 20 product categories (Type C). Companies that wish to conduct self-assessments for compliance must adhere to their category's Type C standards. If everything proceeds as planned, the main standards will be ready by autumn 2026.

CYBER SOLIDARITY ACT

In December 2024, member states adopted the Cyber Solidarity Act to enhance the EU's capacities to detect, prepare for and respond to significant and large-scale cybersecurity threats that affect more than two member states.

The regulation, unveiled in January 2025, includes three key measures: a European cybersecurity alert system for real-time threat detection and response, a cybersecurity emergency mechanism to improve preparedness and response capabilities for large-scale cyber incidents, and a cybersecurity incident review mechanism for analysing major cyber incidents and providing recommendations to strengthen EU cybersecurity.

Last year also saw the adoption of two additional cybersecurity regulations: amendments to the Cybersecurity Act (CSA+), which addresses managed security services, and a regulation setting cybersecurity requirements for cross-border electricity flows.

WHAT TO EXPECT IN 2025

Significant progress was made in cybersecurity regulation last year. In 2025, the EU will begin revising the Cybersecurity Act, which governs the role of the EU agency in charge of cyber security (ENISA) and the EU cybersecurity certification framework. The five-year-old regulation needs updating to reflect ENISA's evolving responsibilities and to improve certification processes in the cybersecurity sector.

The EU will also update its framework for responding to cyber incidents and crises, which was originally developed in 2017. The world has changed significantly since then, and greater focus is needed on preparedness and resilience. The European Commission has started the year actively, unveiling a proposal on 15 January for improving cyber security in the healthcare sector.

While some critics argue that the EU's cybersecurity efforts remain insufficient, most experts advocate for a regulatory pause to allow for the effective implementation of existing measures. Now, the EU and its member states, including Estonia, must focus on enforcing regulations and supporting stakeholders in meeting the new requirements.

How can Estonia shorten ITS CYBER BORDERS?

Over the past decade, the number of state-maintained databases has nearly tripled, significantly extending Estonia's cyber border, which requires monitoring and protection. This digital perimeter can be reduced by adopting centralised services offered by RIA.

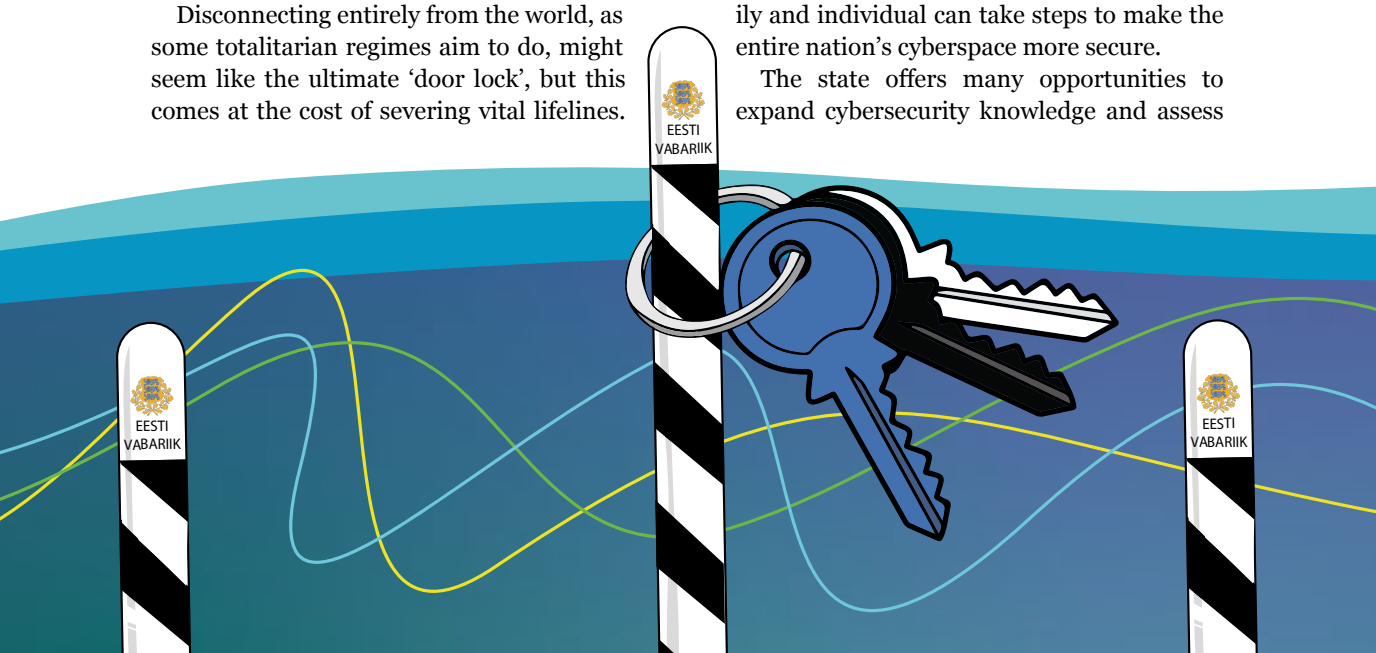
To keep unwelcome, malicious visitors at bay, we typically lock our doors. However, locked doors alone will not deter the most persistent intruders; more sophisticated and intelligent deterrence, prevention and blocking mechanisms are needed. The same mindset applies to ensuring national cyber security.

Disconnecting entirely from the world, as some totalitarian regimes aim to do, might seem like the ultimate 'door lock', but this comes at the cost of severing vital lifelines. In cyber terms, isolation breaks the functionality of countless critical services we rely on daily.

CYBER SECURITY IS EVERYONE'S RESPONSIBILITY

National defence is often viewed as a shared responsibility, and the same should apply to cyber defence. Every institution, business, family and individual can take steps to make the entire nation's cyberspace more secure.

The state offers many opportunities to expand cybersecurity knowledge and assess



one's skills. RIA publishes regular updates on the current climate in cyberspace, describing major incidents to help people learn from other's mistakes rather than making their own. It also provides tools like the Kübertest e-learning platform and the IT-vaatlik prevention portal.

State institutions have access to a range of RIA services designed to keep malicious actors out of state systems, safeguarding the availability of essential services when people need them most.

EXPANDING CYBER BORDERS

However, there is also a flipside. Over the past 10 years, the number of state-maintained databases has grown from approximately 500 to 1,400 – a significant increase in attack surface, nearly tripling the country's exposure to potential threats.

This can be likened to the national border extending threefold, requiring more effective and intelligent measures to monitor and distinguish between malicious activities and legitimate traffic. The annual rise in cyberattacks compounds the challenge, as artificial intelligence drives the growing sophistication of threats.

STRENGTH IN SHARED SOLUTIONS

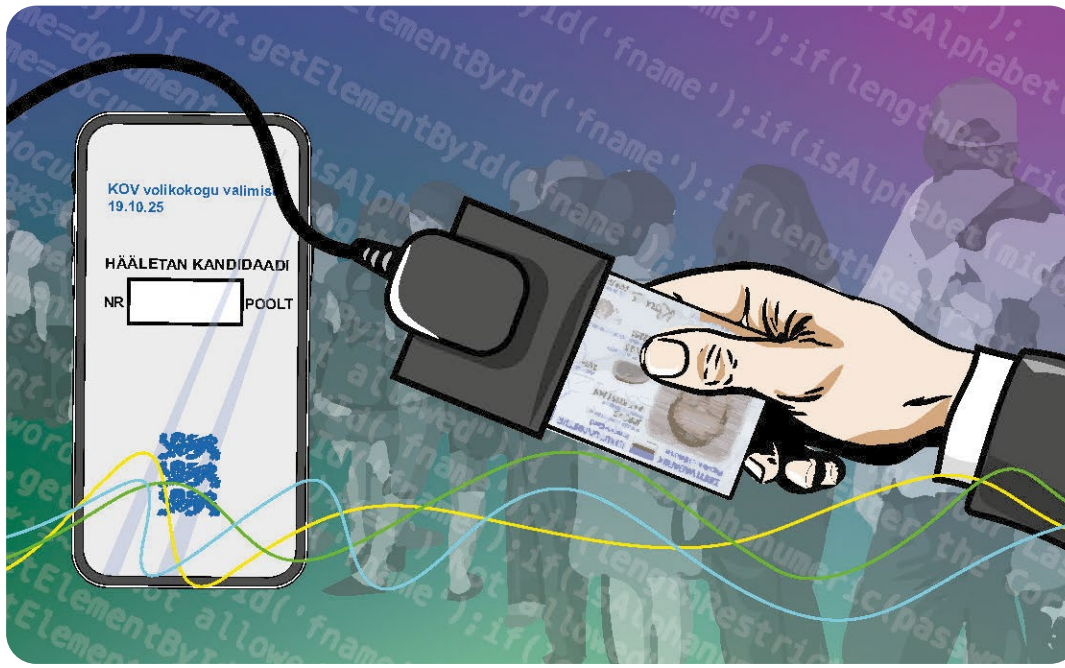
The state has a multitude of institutions, each providing a variety of services supported by extensive IT infrastructure, from traditional servers and networks to bespoke software solutions. Ideally, challenges within this vast and complex system would be resolved once and applied universally. Unfortunately, this is not yet the case.

While one arm of RIA focuses on maintaining traditional cybersecurity, the other develops and provides system components as services to institutions, offering standardised solutions for functions that are fundamentally similar or meet common needs. Examples include the national authentication service, the secure data exchange layer X-Road, the state portal eesti.ee and the national mailbox service. These RIA services cover essential building blocks that individual institutions would find impractical to construct, maintain or operate themselves. Built once, they are designed to serve many – a principle that Estonia strives to uphold.

These RIA services cover essential building blocks that individual institutions would find impractical to construct, maintain or operate themselves.

The widespread adoption of RIA services helps to contract the national cyber border and make its defence more manageable. As a bonus, organisations no longer need to do everything themselves, allowing them to focus on their core responsibilities. Reusing standardised solutions and only developing institution- or business-specific tools free up resources – people, money and time – that can be redirected toward creating greater value for society and protecting it. By reducing quantity, we can enhance quality.





I-VOTING: 20 years of progress

The local government elections in October 2025 will mark the 20th anniversary of i-voting in Estonia.

Last year's Estonian election for the European Parliament went smoothly. The voting process, including internet voting and vote verification, functioned as expected, without any disruptions. Cyber activity during the election week was relatively quiet – no attacks were detected against election systems. Although some web browsers initially flagged the voter application's executable file as malware at the start of election week, this issue was quickly resolved thanks to effective collaboration with Google.

The i-voting platform's reliability was further confirmed by record voter engagement with the verification app: nearly 10% of i-voters checked that their vote had reached RIA's collection server, which is the highest rate to date. The more voters verify their votes, the more certainty election organisers have that the system and voters' devices are uncompromised.

SIX MEDIUM-LEVEL RISKS

Technological advancements have raised new questions about the security of Estonia's e-services. To address these concerns, the Standing Committee on Cybersecurity at the Estonian Academy of Sciences analysed how best to ensure the security of Estonia's e-services, publishing its findings in October.

No high or critical risks were identified in the i-voting system. However, six potential medium-level risks were found, which require ongoing mitigation efforts. These efforts should focus on balancing campaigns that seek to undermine trust in democratic elections, continuously safeguarding the security and reliability of existing voting methods, developing a method to verify the authenticity and integrity of the mobile voter application, improving the i-voting protocol to enhance auditability and transparency, further refining election auditing and observation processes, and strengthening the reliability of election information systems.

> Ultimately, the decision on whether risks have been sufficiently mitigated or deemed acceptable rests with Estonia's National Electoral Committee.

The remaining 25 risks were classified as low, including concerns widely debated in the public sphere, such as the possibility of votes being deleted or altered in the e-ballot box. These scenarios are prevented by built-in system controls that make such tampering impossible.

I-VOTING ON MOBILE DEVICES

Estonia's e-services prioritise user-friendliness and innovation, and i-voting is evolving along the same path as it expands to meet users where they are – on their mobile devices. The prototype of a mobile voting application represents a significant step forward, making i-voting more accessible and convenient.

The technical prototype of the mobile voting application is now complete, having been tested for vote submission, transmission and reception. Ongoing collaboration with technology companies and election organisers aims to mitigate potential risks. Unlike software distribution on computer operating systems, mobile applications are distributed through app stores.

Transparency and auditability are crucial concerns, requiring close cooperation with app store providers such as Google and Apple to ensure the integrity of the application. Ultimately, the decision on whether risks have been sufficiently mitigated or deemed acceptable rests with Estonia's National Electoral Committee.

Roles in election administration

State Electoral Office – Responsible for organising elections, both at polling stations and electronically.

National Electoral Committee – Oversees elections, registers candidates, certifies final voting and election results, handles election-related complaints and violations, and ensures election integrity.

Information System Authority – Acts as a technology and innovation partner for election organisers, which includes managing election-related information systems and maintaining cybersecurity.

I-VOTING MARKS ITS 20TH ANNIVERSARY

The Estonian local government elections will take place from 13 to 19 October 2025. Preparations are in full swing to ensure a smooth and secure electoral process. This election will be a major milestone in the history of Estonia's i-voting system, marking two decades since its first implementation. Over this time, Estonia's i-voting solution has become a model for the world and has shown that technology can enhance electoral processes by increasing both trust and security.

To further strengthen the security of i-voting, several technological upgrades will be introduced in the upcoming elections, such as Smart-ID for voter authentication and the implementation of elliptic-curve cryptography.

What to expect in cyberspace IN 2025



Another record year for cyber incidents

As discussed in this yearbook, Estonia experienced a record number of reported cyber incidents with an impact in 2024. Looking at the latter half of the year, especially the final months and weeks, we anticipate this upward trend will continue into 2025. While the rate of increase may not be as steep, it would be naïve to expect a decline. This continued rise is driven by both the growing capabilities of cybercriminals and increasing public awareness that incidents should be reported to RIA's Incident Response Department at cert@cert.ee or via raport.cert.ee.

An increased likelihood of a major incident

Cybersecurity is never a finished task. As technology evolves, so do the opportunities for criminals and state-backed groups to cause harm – whether for financial gain, espionage or disruption of critical services. In reality, as demonstrated by the destruction of several underwater cables in the Baltic Sea since October 2023, taking down critical infrastructure does not always require sophisticated cyberattack capabilities. Sometimes, all it takes is an ageing vessel with an anchor that fails to stay aboard.

No matter how well RIA prepares to prevent and counter cyber incidents, or how seriously Estonian institutions, businesses and individuals strive to protect themselves, the attacker always holds the advantage. Suppose we imagine Estonia's cyberspace as a sprawling summer meadow, alive with blooming flowers,



birdsong and children at play. In that case, we must also picture a high fence meant to shield it from malicious intruders. This fence must be impenetrable at every point, requiring constant vigilance from defenders across the entire perimeter.

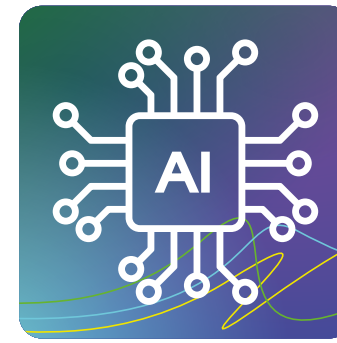
Meanwhile, the attackers need only a single ladder to climb over or one tool to break through. Under these conditions, the question is not if a serious incident will occur, but when.

Growing awareness of China's role in cyber security



In the final months of 2024, several news stories in Estonia highlighted China's influence, including its implications for cyber security. One widely discussed topic was whether the city of Tallinn should use TikTok, a platform controlled by the Chinese government – this later evolved into a broader debate on whether Estonia should ban TikTok, which helps train China's artificial intelligence systems. Another major issue was the arrival of Chinese BYD electric vehicles into the Estonian market, with concerns that their data is transmitted to servers in China, where authorities have access. Discussions also arose over whether Chinese-made routers are secure and should be used. These debates paralleled questions raised in September about members of the Estonian Parliament's China Friendship Group, some of whom travelled to China on visits partially funded by the Chinese state. All of this unfolds against the broader backdrop of China's close ties with Estonia's eastern neighbour, its stance on Russia's aggression against Ukraine and its military manoeuvres around Taiwan.

China's role in cybersecurity will not fade in 2025 – or beyond. We expect growing awareness of these red flags to influence consumer and policy decisions. When products from a particular country systematically transmit user data to that country's authorities – and when that country stands on the opposite side of major global value divides from Estonia and its allies – it is worth thinking twice before buying the latest Chinese gadget or letting children install TikTok on their phones.



AI continues to grow

Artificial intelligence is advancing at an extraordinary pace. In addition to more sophisticated phishing emails, cybercriminals now use AI applications to generate attack codes. In hindsight, it has also become clear that AI-generated code was used in attacks against Estonian heating plants and water stations during the wave of cyber incidents following the outbreak of the Israel-Hamas conflict at the end of 2023. One of the world's best-known artificial intelligence developers, OpenAI, reported in October 2024 that its AI-powered chatbot, ChatGPT, had been used to prepare cyberattacks, including for developing malware, spreading disinformation and producing phishing messages. The report specifically mentioned China, Iran and Russia. Of course, AI is also being harnessed for defence.

Another major data breach on the horizon?



Data protection was also featured in last year's cybersecurity forecast, following several significant data leaks in 2023. At the time, we expressed hope that public exposure of these cases would encourage institutions and companies to improve their ability to protect the personal data entrusted to them. However, just days after the publication of our 2024 yearbook, RIA learned of yet another – and by far the largest – personal data breach in Estonia, details of which are covered in this edition. Fortunately, Estonia has seen no further large-scale violations since then, but there is no reason to assume that the most recent one will be the last.

Cyber Security in Estonia 2025

Publisher: **Information System Authority**
Pärnu mnt 139a, 11317 Tallinn
Design: **Martin Mileiko** (Profimeedia)
Illustrations: **Andres Varustin**
Translation: **Margus Elings** (Refiner)
Editing: **Scott Abel** (Tekstikoda)



Read more: **www.ria.ee/en**