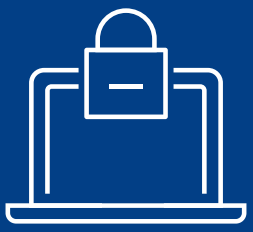
Republic of Estonia
Information System Authority








CYBER SECURITY IN ESTONIA 2026

REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Cyber Security in Estonia 2026

CONTENTS

FOREWORD

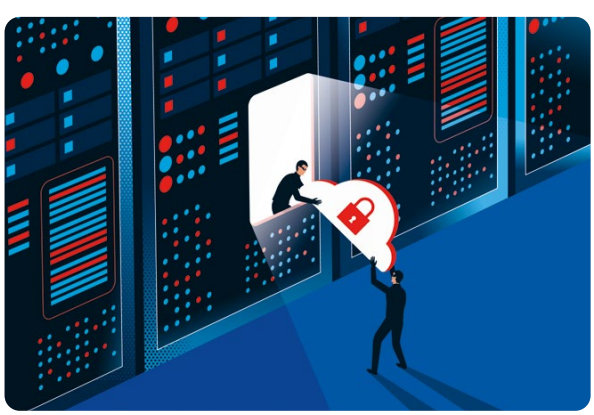
6 **Trust that endures**
Amid escalating threats and a deepening reliance on digital solutions, our resilience is shaped by how deliberately we manage risks and sustain trust, writes **Gert Auväärt**, Deputy Director General for Cybersecurity at RIA.

OVERVIEW OF 2025

8 **Cyberspace in 2025: a year of scams**
Cable faults, service outages and denial-of-service attacks were more frequent than expected in 2025. Above all, however, the year will be remembered for the record number of scams and the damage they caused.

14 **DDoS attacks: new groups target Estonia**
Groups originating in the Middle East, North Africa, and South-East Asia also began targeting Estonia.

16 **Ransomware: new attacks, familiar mistakes**
The number of ransomware attacks and the damage they cause continue to rise globally. In Estonia, the situation remains relatively stable, but we have also seen attacks that have led to serious disruption.



18 **A surge in scams costs people in Estonia €29 million**
While warning signs had appeared earlier, 2025 saw the collapse of the language barrier that had previously offered at least some protection against scams.

22 **2025 saw another record number of vulnerabilities**
Serious vulnerabilities were found in network devices, industrial automation systems, operating systems and a wide range of other software.

24 **The global cyber landscape in 2025**
Ransomware attacks battered the reputations of well-known brands, North Koreans using fake identities attempted to infiltrate international technology companies, and large-scale service outages exposed critical dependencies.

28 **War in Ukraine's cyberspace: the defence holds**
For the first time since the start of Russia's full-scale invasion, Ukraine did not experience a cyberattack with a major societal impact in 2025.

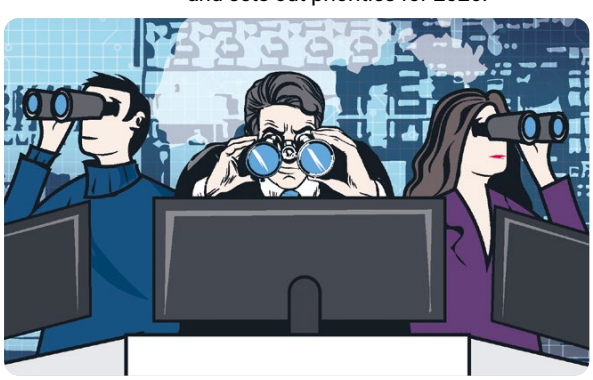
30 **SSSCIP chief: A peace deal won't bring peace in cyberspace**
Brigadier General **Oleksandr Potii**, head of Ukraine's State Service of Special Communications and Information Protection (SSSCIP), speaks about developments in Ukraine's cyberspace over the past year and what others can learn from them.

32 **Cyber menu 2025: Peking duck**
Data leaks have given us a glimpse into China's offensive cyber ecosystem, which is characterised by extensive cooperation between the private sector and the state.

36 **Russian bears in cyberspace**
Russia uses cyberspace as a targeted and effective tool to support its foreign and security policy objectives.

SAFER CYBERSPACE

40 **The ministry's perspective: developments and next steps**
Tõnu Grünberg, Deputy Secretary General for digital infrastructure and cybersecurity at the Ministry of Justice and Digital Affairs, looks back on developments in national cybersecurity over the past year and sets out priorities for 2026.



42 **20 years of protecting Estonia's cyberspace**
We look back on the eventful history of Estonia's incident response team CERT-EE.

46 **RIA operations centre begins work**
On 1 June 2025, RIA launched its operations centre, tasked with observing and managing the operation of RIA services and monitoring developments in Estonia's cyberspace.

48 **What did we do in prevention?**
In 2025, our largest prevention campaign targeted businesses, helping them recognise cyber threats and protect themselves.

50 **How to make public services more resilient**
Estonian society relies on convenient public services, but behind them lies a web of dependencies. RIA identifies and strengthens the weakest links in this system to ensure that services continue to function even when a critical communications cable or power connection fails.

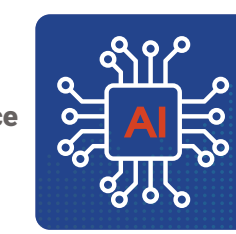
52 **"In the worst case, we could be without electricity for days"**
These ominous words were heard during the Cyber Reserve 2025 exercise, where participants, working with Elering, practised responding to a cyberattack that threatened Estonia's entire electricity supply.

54 **Cybersecurity reflects organisational maturity**
Cybersecurity is often framed in technical terms, but these form only part of the picture.

56 **New grant for cybersecurity companies**
RIA and the Estonian Business and Innovation Agency (EIS) have created a new innovation grant for cybersecurity companies to support product and service development in the sector.

58 **EU CyberNet expands its reach**
The European Commission has extended EU CyberNet, the EU-funded cybersecurity capacity-building project led by RIA, for a further three years. This brings new partners and opens up opportunities to deliver EU assistance in South-East Asia and the Indian Ocean region.

60 **What to expect in cyberspace in 2026**



TRUST THAT ENDURES

Amid escalating threats and increasing reliance on digital solutions, our resilience is shaped by how deliberately we manage risks and sustain trust – at every level, from the state and organisations down to individual citizens, writes **GERT AUVÄÄRT**, Director of the National Cyber Security Centre, NCSC-EE.

Cybersecurity is what keeps everyday life running. It is the backbone that ensures the lights turn on, water flows from the tap, bank transfers go through, and payments can be made in shops. Most of the time, we do not think about it – and that is exactly how it should be. The strength of Estonia's digital state lies not only in smart services but in their quiet reliability, even when cyberspace is turbulent and technology unpredictable. This invisible continuity is a pillar of modern society.

Developments over the past year have made it clear that cybersecurity is no longer a niche concern for IT enthusiasts. It underpins how society functions, shaping business, public services, energy security and people's everyday sense of safety. The functioning of the digital state is inseparable from the stability of cyberspace, and any disruption or attack can have consequences that extend far beyond a single system or service.

Developments over the past year have made it clear that cybersecurity is no longer a niche concern for IT enthusiasts.

THREATS THAT STRIKE WITHOUT WARNING

Cyber threats worldwide are growing in scale and sophistication. Zero-day vulnerabilities are exploited within hours, ransomware attacks inflict direct financial losses while corroding trust, and state-backed threat actors operate with a long-term view, seeking persistent access to critical systems. At the same time, advances in artificial intelligence are making attacks faster and harder to detect. Responding after the incident is no longer enough – continuous situational awareness and preventive readiness are now essential.

Cyber threats are also affecting ordinary people more directly. For victims of fraud, the damage extends beyond money, eroding their sense of security and confidence. Last year brought this into sharp focus: people in Estonia lost 29 million euros to fraudsters. The disappearance of language barriers and the skilful use of social manipulation have made fraud pervasive, particularly through phone calls that exploit urgency, fear and perceived authority. This shows that the security of the digital

Gert Auväärt

state depends not only on technical solutions but also on the decisions people make when their trust is deliberately manipulated.

PREVENTION BEGINS WITH DECISIONS

In this environment, the key question is how we collectively understand and mitigate risks. A large share of cyber incidents remains preventable through better cyber hygiene and well-considered management decisions. An organisation's level of cybersecurity reflects its maturity, sense of responsibility and willingness to confront uncomfortable scenarios honestly.

Not all major digital disruptions, however, are the result of malicious attacks. The most extensive global outages in 2025 stemmed from technical failures at major cloud service providers, simultaneously affecting thousands of organisations and millions of users. These incidents exposed just how tightly our everyday lives and economic activity are bound to a small number of critical global providers.

The strength of a digital state is measured by its capacity to innovate and, crucially, by its ability to remain functional when things go wrong. Achieving a unified view and stronger preparedness requires a comprehensive picture. A significant step in this direction was the establishment of RIA's operations centre, which brings together situational awareness of developments in Estonia's cyberspace and the status of national critical services. This shared awareness enables faster responses, closer cooperation and clearer leadership.

CYBERSPACE KNOWS NO BORDERS

All these themes are tied together by a single underlying principle: cybersecurity is, above all, a matter of leadership, responsibility and cooperation. Technologies and standards are indispensable, but they are not sufficient on their own. A responsible state understands its risks and prepares for uncomfortable scenarios.

Estonia's experience and expertise are also needed – and valued – internationally. Cyberspace has no borders, and a weak link elsewhere can quickly affect others. International cooperation, information sharing and joint exercises are essential to building resilience.

This invisible yet critical resilience is perhaps most clearly seen in CERT-EE's 20-year journey. It is a story of continuity and persistence that rarely attracts public attention but keeps services running, crises at bay and trust intact.

Our shared goal is a resilient Estonian state: one where the lights turn on, water keeps flowing, and digital services continue to function.

Our shared goal is a resilient Estonian state: one where the lights stay on, water keeps flowing, and digital services continue to function – and where trust, our greatest and often least visible capital, remains secure.

Cyberspace in 2025: A YEAR OF FRAUD

Cable faults, service outages and denial-of-service attacks all occurred more often than expected in 2025. Above all, however, the year will be remembered for the record number of scams and the damage they caused.

Cases drawn from reports by the Police and Border Guard Board and RIA could fill an entire book:

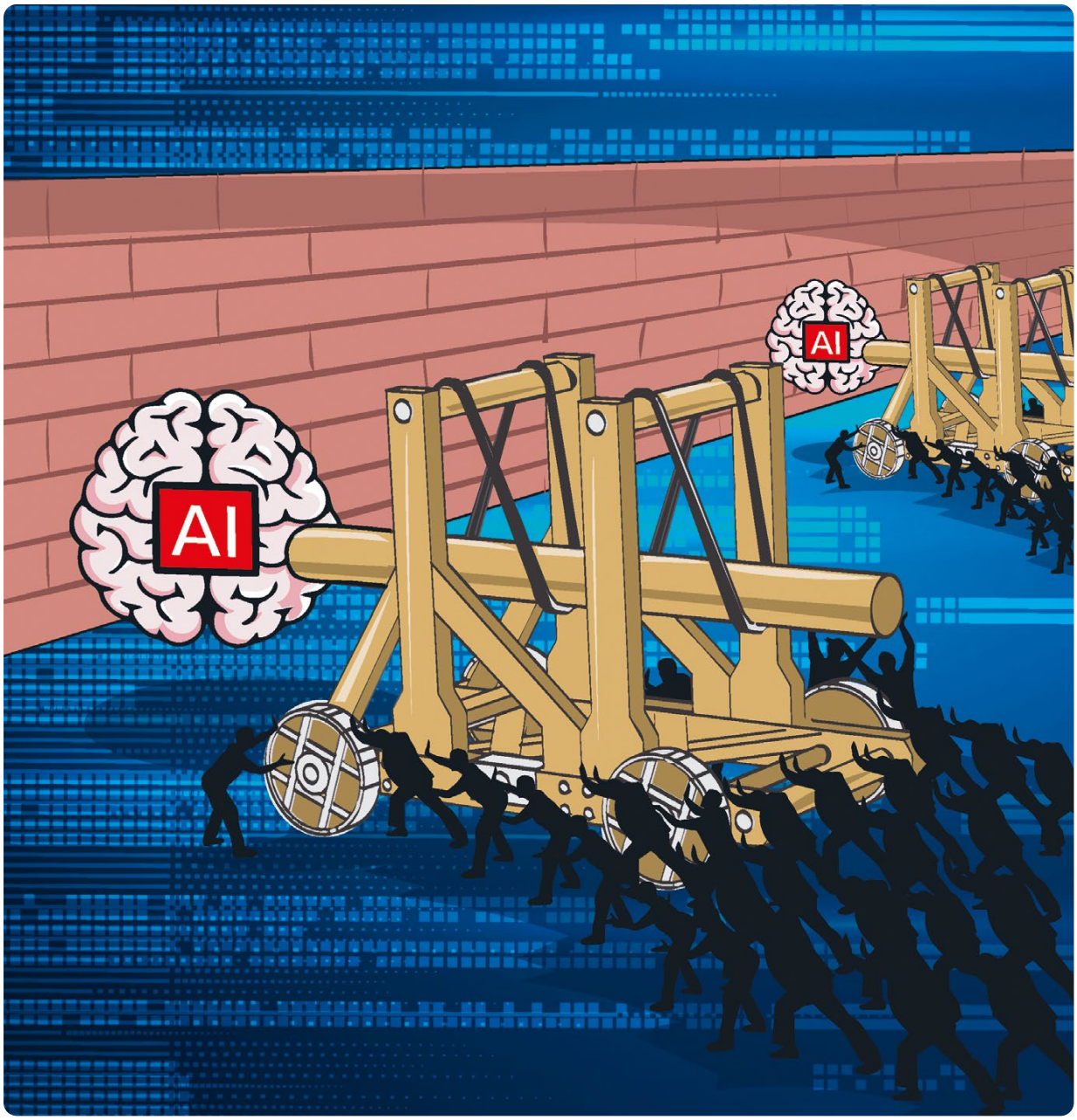
- A 57-year-old man was contacted by a person presenting themselves as an investment adviser. Acting on the adviser's guidance, he registered on a cryptocurrency trading platform and made an initial deposit of 1,300 euros. Over the next six months, following the fraudsters' instructions, he transferred funds from his company's accounts to the fake platform, totalling 504,400 euros.
- A 54-year-old woman met a stranger on Messenger. After a few days of conversation, the man steered the discussion towards investing and advised her to register on an investment platform. At the scammers' urging, the victim took out loans over a five-month period and handed over cash and gold so that the scammers could deposit the funds on the platform. She also sold her apartment and gave the proceeds to a courier. The scam resulted in losses of at least €200,000, based on initial estimates.
- A 71-year-old woman received calls from scam-

JANUARY ›

- Denial-of-service attacks target a bank operating in Estonia, causing brief disruptions to its online services.
- Phishing emails and messages circulate in the name of the Estonian Tax and Customs Board, claiming that recipients are entitled to a tax refund. Users are prompted to scan a QR code that leads to a phishing website.
- The automated border control (ABC) gates stop working due to an expired certificate.

FEBRUARY ›

- At the beginning of the month, Mobile-ID experiences disruptions in Elisa's network, and at the end of the month, in Telia's network.
- Disturbances in the emergency alert system cause longer-than-usual wait times for some 112 calls.
- The Eesti.ee application is unavailable for more than 24 hours.



MARCH ›

- Denial-of-service attacks targeting a bank's name servers disrupt its online banking, mobile app, and instant payment services.
- Login disruptions affect systems within the Ministry of the Interior's area of government, including those of the Police and Border Guard Board and the Emergency Response Centre.
- Smart-ID experiences service disruptions.

APRIL ›

- At the beginning of the month, Estonia faces a large wave of denial-of-service attacks. The attacks are more technically complex than usual, resulting in brief outages on some websites.
- Scam phone calls spread in which fraudsters pose as Health Insurance Fund employees and persuade victims to enter their Smart-ID PIN codes.

➜

mers posing as the police and a bank. Following their instructions, she sold two apartments she owned, withdrew the proceeds in cash and handed the money over to strangers. The estimated loss in this case amounts to 138,000 euros.

Taken together, the losses from just these three cases in Estonia total nearly one million euros, with all fraud-related losses recorded in 2025 amounting to 29 million euros.

Previously, the language barrier offered at least some protection. In 2025, that defence collapsed.

AN ENDLESS AVALANCHE

That sum exceeds the annual budget of the resort town of Haapsalu in western Estonia. It would have been enough to build a new state secondary school or to buy several new trains for the national rail operator Elron. By contrast, the national broadcaster ETV's annual charity programme Jõulutunnel, raised less than 400,000 euros to support the treatment of children with rare diseases, while scammers took in tens of millions.

Previously, the language barrier offered at least some protection. In 2025, that defence collapsed. Estonian speakers have been recruited by foreign call centres that run scams. A single scam now often involves two or three fluent Estonian speakers: one posing as, for example, a Health Insurance Fund employee, another as a bank official and a third as a police officer.

The scenarios vary – replacing an electricity meter, an investment scheme promising exceptional returns, an unclaimed benefit or something else entirely – but the outcome is the same. By entering PIN codes during a call, handing over bank card details or transferring money to a fraudulent platform, victims part with their savings. The chances of recovering that money are almost non-existent.

So far, phone scams have been carried out by real people. Given the pace at which artificial intelligence is learning Estonian, however, we will very likely start receiving calls from machines in the coming years. At least initially, AI may not be as persuasive as a human, but quantity can compensate for quality.

AI has already been used for some time to generate phishing emails, messages and websites. The increase in volume has been striking: in 2025, we detected more scam websites than ever before, mostly masquerading as online shops or investment platforms. Once such pages are discovered, we ask hosting providers to remove them, but new ones appear just as quickly.

Although an informed and cautious public remains the most critical line of defence, technical measures can also significantly constrain scammers' operations. For phone users, the Encrypted DNS application developed by CERT-EE helps block access to known malicious websites where users risk losing money or personal data.

MAY ›

- During maintenance work on East Tallinn Central Hospital's IT systems, a fault occurs that prevents servers from accessing necessary data. A crisis situation is declared: surgeries are postponed, and patients arriving at the emergency department are redirected to other hospitals. Network services are restored after 2.5 hours.

JUNE ›

- During maintenance work, the external connections of the Health and Welfare Information Systems Centre (TEHIK) are interrupted, affecting dependent services: the health information system, Health Insurance Fund services (digital prescriptions, insurance status checks and incapacity benefits), the health portal, and TEHIK's website.
- A fault in an administrative system disrupts many systems in the Ministry of the Interior's area of government. As a result, waiting times for emergency calls and queues at border crossing points are longer than usual. Document issuance at Police and Border Guard Board offices and Selver stores is interrupted.

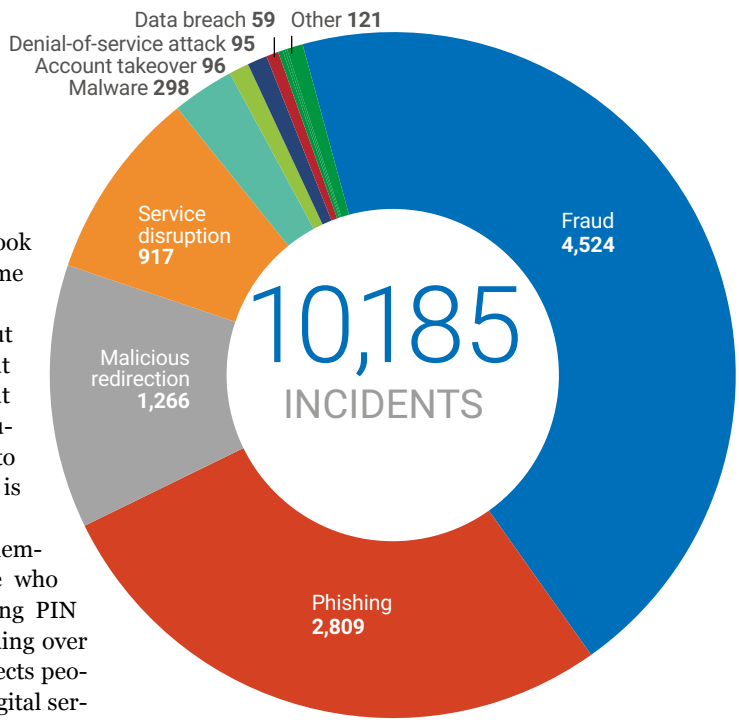
In addition, SK ID Solutions introduced an updated version of its Smart-ID authentication tool, marketed as Smart-ID+. While it is no silver bullet against all scams, it is expected to slow down some phone scams that pressure users to enter PIN codes.

No one should lower their guard. When one opportunity closes, scammers look for the next, and it would be naïve to assume they will not find one.

Why do we write and talk so much about scams? 29 million euros is a large sum, but the issue is not only money. It is also about trust and the public's general sense of security. How safe people perceive cyberspace to be depends mainly on how freely crime is allowed to operate there.

Even if they have not been affected themselves, almost everyone knows someone who has fallen victim to a scam – by entering PIN codes when they should not have or handing over bank card details or money. All of this affects people's sense of security and their trust in digital services generally. You can read more about scams on page 18.

INCIDENTS WITH IMPACT IN 2025



GEOPOLITICAL ECHOES IN ESTONIA'S CYBERSPACE

Russia's full-scale war against Ukraine, launched in 2022, led to a sharp increase in denial-of-service attacks against Estonia. This is no longer news – we have covered it in the past three annual reports. Nor was 2025 an exception. In 2025, the number of denial-of-service attacks reached yet another record, but attackers enjoyed little success: for the second year in a row, the number and share of attacks that had any impact at all – usually a brief disruption to a website or service – declined.

There were, however, some surprises. While Estonia had previously been a favoured target of pro-Kremlin hacktivists angered by our support for Ukraine, last year also brought attacks by pro-

JULY ›

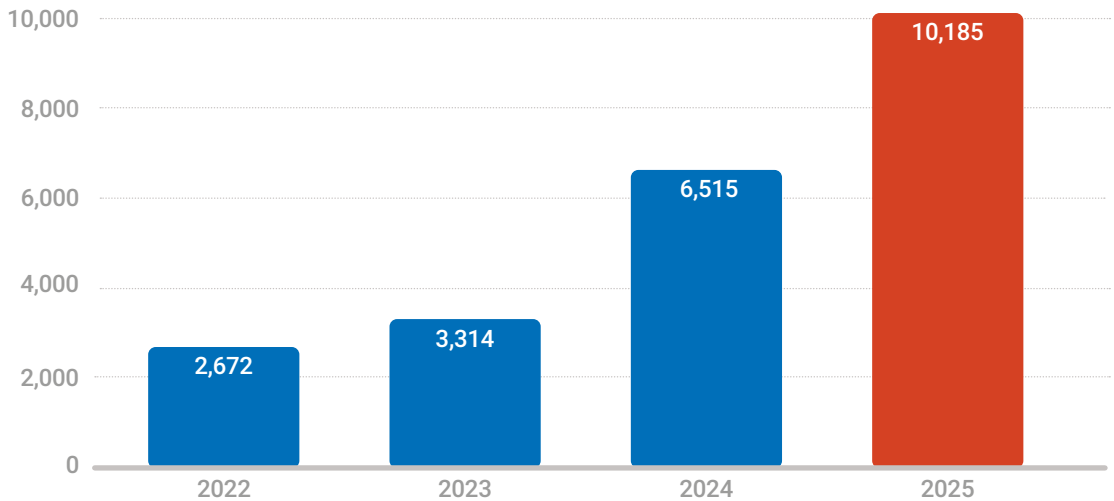
- The emergency call handling information system malfunctions again. Emergency response centres revert to pen and paper, slowing work and causing call queues.
- Mobile-ID experiences several disruptions. In at least two cases, the cause is a denial-of-service attack.
- In the Eesti.ee application, queries related to identity documents and other services fail. A sudden surge in users reveals a configuration error that did not appear under a lighter load.

AUGUST ›

- The engineering company Hekotek's loss of more than 1 million euros to scammers becomes public. The chain of events began with a scam call to the company's chief financial officer, in which fraudsters pose as Health Insurance Fund employees.
- Phishing emails circulate in the name of Elisa and Telia. Emails sent in Elisa's name claim that customers have overpaid and request payment details for a refund. Emails sent in Telia's name claim an outstanding bill and direct recipients to a fraudulent payment link.

→

NUMBER OF INCIDENTS WITH AN IMPACT DOUBLED



Palestinian groups from the Middle East, North Africa and Southeast Asia.

Their most notable campaigns took place in April and May. These attack waves were large in scale and more complex than average, with attackers continuously adjusting their tactics in an attempt to circumvent defensive measures.

You can read more about denial-of-service attacks, their impact and the reasons Estonia became a target for pro-Palestinian groups on page 14.

NOT EVERY INCIDENT IS AN ATTACK

While denial-of-service attacks caused disruptions or outages in 95 cases, incidents arising from other causes were almost ten times more numerous. In most instances, these were not the result of malicious intent or deliberate planning but stemmed from human error, configuration issues, or software and hardware faults.

Last year did not bring service outages that shook society as a whole, but more minor inconveniences were frequent. In May, telecommunications provider Elisa experienced disruptions to its voice services. In June, some Telia customers in Lääne-Viru County were affected. Estonian Health Insurance Fund services, such as digital prescriptions and insurance status checks, experienced repeated disruptions, and on several occasions, the automated border control gates (ABC gates) stopped working. There were also faults affecting

SEPTEMBER ›

- Train ticket sales on Elron's website are interrupted twice. In both cases, the cause is an error in Ridango's systems, which operate the ticketing platform.
- Disruptions affect the services of Swedbank (online banking, app and card payments), Luminor (card payments) and SEB (website).
- Phishing messages circulate in Omniva's name, and scam emails circulate in Telia's name.

OCTOBER ›

- Local government council elections pass with relatively few incidents. Denial-of-service attacks target election-related websites, but these have no impact.
- The population register services malfunction, disrupting dependent services, such as emergency call handling and identity document services.
- Various phone and online scams resurface. A large share of scam calls are made in the name of Elektrilevi and the Health Insurance Fund, offering to replace electricity meters or reimburse healthcare costs.

internet banking, Mobile-ID and Smart-ID. On multiple occasions, passengers were unable to purchase train tickets on Elron's website due to issues with Ridango's systems, which manage the ticketing platform.

Cybersecurity should be layered, like a millefeuille.

The most visible incidents, however, were two service outages whose causes lay outside Estonia, in the United States. On 18 November, a failure at Cloudflare – a global internet infrastructure and security company whose services are widely used in Estonia – led to widespread disruption. For several hours, major news portals (Delfi, Eesti Ekspress and Õhtuleht) were unavailable, while the websites of long-distance coach operator Lux Express and rail operator Elron were also affected, preventing ticket purchases.

An outage of this scale at a company on which a large share of the world's internet depends is rare. Even more unusual was the fact that a similar incident occurred less than three weeks later. This time, many public-sector websites in Estonia were affected, including those of the parliament, the government and the police. Bolt's website and app were unavailable, and disruptions to the national authentication service TARA lasted about 20 minutes.

In the first case, the outage was caused by an error during a database update. In the second, a firewall change did not proceed as intended.

The year ended with further reports of problems affecting undersea cables. On 28 December, faults occurred in the Citic Telecom data cable between Estonia and Sweden. On 30 December, problems affected Telia's cable connecting the island of Hiiumaa with mainland Estonia, as well as Arelion's cable between Hiiumaa and Sweden. On the final day of the year, damage was reported to two cables connecting Estonia and Finland, one operated by Elisa and the other by Arelion. Investigations are ongoing, but the incidents did not result in major service disruptions, as data traffic was rerouted through alternative connections.

This is how all services – and our cyber defence – should work. If one connection or data centre goes offline due to a fault or an attack, service provision should quickly switch to a backup solution. Cybersecurity should be layered, like a mille-feuille. If the first layer fails to stop an attacker and a phishing email recipient clicks on a link, the second layer – background software – should block the connection to the phishing site before the user has a chance to enter their details. Layered defence and services with robust backup solutions are essential.

The year ended with further reports of problems affecting undersea cables.

NOVEMBER

- A Cloudflare outage causes disruptions in many countries, including Estonia. For several hours, the news portals Delfi, Eesti Ekspress and Õhtuleht, as well as etv.ee and vikerraadio.ee, are unavailable. The websites of Lux Express and Elron are also disrupted, preventing ticket purchases, and Enefit's website is affected as well.
- Denial-of-service attacks target the websites of Tallinn and Tartu, causing brief outages and slowdowns.

DECEMBER

- Cloudflare systems malfunction again. Many public-sector websites are unavailable, including those of the parliament, the government and the police. The national authentication service TARA and Bolt's applications are also disrupted. In Estonia, the outage lasts about 20 minutes.
- A family medical centre reports that it has been hit by a ransomware attack. Data on two servers, as well as backups, are encrypted. The affected servers contain patient data, medical records and appointment schedules, paralysing the centre's operations.
- Train ticket sales on Elron's website are interrupted once again.

DDOS ATTACKS: new groups target Estonia

Since 2022, many denial-of-service attacks against Estonia have been carried out by Russian hacktivists. Last year, however, groups originating in the Middle East, North Africa, and South-East Asia also began targeting Estonia.

Let us start with the bad news. The number of distributed denial-of-service (DDoS) attacks targeting Estonia continued to climb in 2025, reaching a record 756. This is more than a third higher than in 2024 and almost as many as in 2022 and 2023 combined.

The good news is that RIA's DDoS protection services proved resilient. Despite the sharp rise in activity, the number of attacks with a tangible impact actually declined. Of the several hundred DDoS attacks recorded during the year, fewer than one hundred caused any harm to the targeted services, typically resulting in a short outage or reduced performance. As a result, attacks with an impact accounted for just 12.5 per cent of the total. This marks a significant improvement compared with 2024, when nearly every fifth attack was successful from the attackers' perspective, or 2023, when the share of attacks with an impact stood at 27 per cent.

A key development last year was not only the growth in attack volumes and technical complexity but also the broadening range of attackers. Since 2022, many of the DDoS attacks against Estonia have been carried out by Russian hacktivist groups, but from early 2025, pro-Palestinian groups from the Middle East, North Africa and South-East Asia also began targeting Estonia's cyberspace.

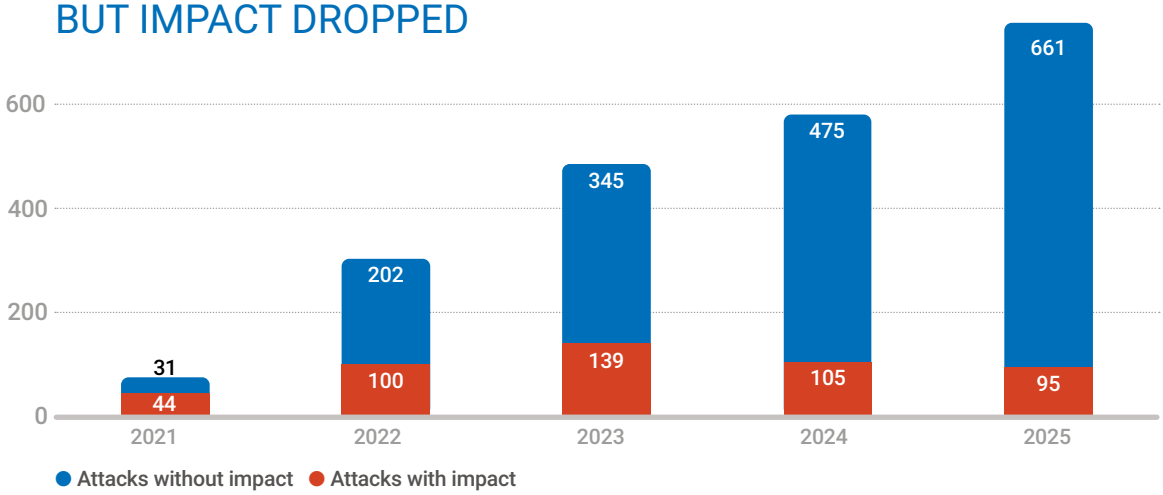
WHAT IS A DDOS ATTACK?

A distributed denial-of-service (DDoS) attack is a cyberattack aimed at making a targeted digital service – such as a website, e-service, information system or network service – unavailable to users. The attacker sends an extremely large number of requests towards the target (a server, network device or intermediary system) from many different devices within a short period of time. As a result, the service is unable to handle regular traffic and becomes wholly or partially unavailable.

WHY ESTONIA?

In terms of methods and motives, pro-Palestinian hacktivists resemble their Russian counterparts. In both cases, attacks are inherently destructive and directed against states they regard as ideological

DDOS ATTACKS INCREASED, BUT IMPACT DROPPED



adversaries. Their campaigns are often aimed at critical infrastructure and seek to cause as much disruption and inconvenience as possible for the population of the targeted country.

In general, hacktivist activity is limited to DDoS attacks and simple compromise attempts. These attacks do not necessarily require advanced technical skills but can generate fear or confusion among the public and draw attention to the attackers.

While Russian hacktivists view Ukraine as their primary ideological target, with countries supporting Ukraine – mainly EU and NATO member states – seen as secondary adversaries, pro-Palestinian groups regard Israel as their principal adversary. Their secondary targets include states and institutions perceived as supporters of Israel. Estonia came into the focus of pro-Palestinian hacktivists largely because it is seen as part of the broader Western coalition.

Another important factor is the active cooperation between Russian and pro-Palestinian hacktivist groups. Although their primary targets differ, their interests overlap when it comes to EU and NATO member states. As a result, pro-Palestinian hacktivists often join attack campaigns against Europe initiated by Russian groups, and countries that have no direct connection to the Israeli–Palestinian conflict can also become targets.

ATTACKS AGAINST ESTONIA

The most significant attack campaigns by pro-Palestinian hacktivists against Estonia took place in April and May 2025. These were the largest and most disruptive DDoS attacks against the country during the year.

In April, a pro-Palestinian group originating from Algeria targeted Estonia's cyberspace, carrying out three large-scale attack campaigns against websites in both the public and private sectors. Across the three waves, RIA identified 44 DDoS attacks, 20 of which disrupted services on the targeted websites. These were large-scale attacks of above-average technical complexity: after each wave, the hacktivists adjusted their tactics in an attempt to bypass defensive measures. Within three hours, they sent more than half a billion requests towards 15 targeted websites. In just 11 minutes, 84 million malicious requests were directed at a single website – a volume that would take almost 34 years to accumulate under normal conditions.

In May, a group from Morocco attacked the websites of Estonia's security authorities. RIA identified ten attacks from this group, blocking nearly 225 million malicious requests. Compared with the April campaign, this was around half the total volume but notable for its intensity: these almost quarter of a billion requests were generated within just 39 minutes, meaning the May campaign was almost twice as intense as the April attacks.

Despite the scale and intensity of these campaigns, RIA's DDoS protection blocked the majority of malicious traffic and prevented any tangible impact.

RANSOMWARE: new attacks, familiar mistakes

The number of ransomware attacks and the damage they cause continue to rise globally. In Estonia, the situation remains relatively stable, but we have also observed attacks that led to serious disruption.

A brief outage of a company's or institution's website is nothing unusual. This is often caused by a configuration error, an expired certificate or a hardware failure. For one Estonian company that contacted us, however, it was the first sign of something far more serious. They had fallen victim to a ransomware attack.

WEAK SECURITY POLICY

What most likely began with a company executive's password being exposed in a data leak escalated into an organisation-wide incident.

Several factors contributed to the attack. The executive's home network was part of the company's internal network, and a Remote Desktop Protocol (RDP) connection to the company's servers was saved on the desktop of their personal computer. Convenient, but dangerous.

The company's password policy also proved fatal, as the same passwords were reused across work and personal accounts. Using the same password across all servers no doubt made the attackers' task significantly easier.

In addition to the executive's personal network

storage, the attackers encrypted the company's server logs and backups, which were located on the same network. Fortunately, the company was able to continue operating because business-critical processes were not disrupted; however, restoring the systems took weeks.

OUTDATED SOFTWARE

In the case of another company that fell victim to ransomware last year, we identified the cause as a vulnerability in server software. This flaw allowed malicious code to be executed, enabling the attackers to create a new user account and maintain continued access to the server. Although the software was later updated to a secure version and malicious scripts were removed, the attackers retained access and subsequently sold that access on. The new attackers entered the system using remote administration software, encrypted the data and left a ransom demand on the victim's desktop. Due to backups, the server could be restored, and the company's operations could resume.

Due to backups, the server could be restored, and the company's operations could resume.

A REPEAT INCIDENT

An Estonian logistics company first encountered a ransomware attack a few years ago. It is said that lightning does not strike the same place twice, but in 2025 they once again fell victim to a similar attack.

The attack method followed a familiar pattern. The intrusion was possible because a remote desktop application was openly accessible from the internet. A weak password was also in use and was cracked using a brute-force attack. The attackers then deployed a tool that harvested passwords and user data, allowing them to access other systems as well. Finally, the attackers encrypted the data stored on the company's server. Because critical processes were unaffected, the company was able to continue its work.

THREE ROOTS OF EVIL

Although each case is different, ransomware attacks share common characteristics. The following factors commonly increase exposure to attacks and make system recovery more difficult:

- **Remote Desktop Protocol** (RDP) applications are visible and accessible to the entire internet via public IP addresses.
- **Weak password policies are in place.** Passwords such as Admin, Password123, and qwerty are commonly used and can be easily guessed via brute-force attacks.
- **Backups are missing or are located in the same network.** When attackers encrypt a company server, the backups can be encrypted as well.

AN ATTACK PARALYSED A MEDICAL CENTRE

At the end of the year, a family medical centre reported having fallen victim to a ransomware attack. During the incident, attackers encrypted backups and data on two servers. The most recent backup they could access dated back to 2021. As the attackers managed to lock patient data, medical records and appointment schedules, the medical centre's operations were brought to a halt.

While several hypotheses exist regarding how the attack became possible, the most likely explanation is that a former employee's account was not closed after their departure. The attackers were able to act so extensively because all users in the system had administrator rights. Experts were able to restore only part of the encrypted data.

HOW TO PROTECT YOURSELF

To avoid falling victim to an attack and to minimise damage, use unique passwords and, where possible, implement multi-factor authentication. Hide remote desktop connections from the public network and from personal devices. Review your data backup arrangements. Regularly update device software to prevent the exploitation of vulnerabilities. Consult the cybersecurity quick guide for companies at itvaatlik.ee.

A surge in scams costs people in Estonia 29 MILLION EUROS

While warning signs had appeared earlier, 2025 saw the collapse of the language barrier that had previously offered at least some protection against scams. The result: people in Estonia lost 29 million euros to fraudsters – three times more than the year before.

Scams remained in the public eye for almost the entire year. The media published hundreds of articles, while RIA, the Police and Border Guard Board, banks and many other organisations ran campaigns and awareness initiatives on how to recognise scams and protect oneself. Despite this, fraudsters walked away with larger gains than ever before, and scams account for the largest share of all the incidents registered by RIA. Individuals are most frequently targeted, but by loss amount, business-related fraud causes the most significant financial damage.

MORE CONVINCING SCAMS

Scammers are becoming ever more convincing and sophisticated. Where fraud could once be spotted through poor Estonian grammar or the use of Russian, these clues can no longer be relied on. Today, we see scams carried out in fluent Estonian, making them increasingly difficult for unsuspecting victims to recognise. The best defence is to stay informed about scams currently in circulation.

As in previous years, phishing messages purporting to be from postal and delivery service providers continued to spread widely. Alongside these, however, phone scams increased sharply, affecting both private individuals and company representatives. Scams targeting businesses often result in losses of hundreds of thousands of euros, with little chance of recovery.

PHONE SCAMS SURGED

Every day, people in Estonia lose tens of thousands of euros to phone scams. One common scheme involves a sequence of calls. In the first, the victim is pressured to act quickly – for example, by being offered the return of a supposed compensation payment. In the second call, the caller claims the first call was from fraudsters and that immediate action is needed to stop them, requiring the victim to log in to their bank and confirm this by entering their Smart-ID or Mobile-ID PIN.

Calls claiming that an electricity meter or switchboard needs to be replaced are also common. One non-profit organisation fell victim to such a scheme. The first fraudster introduced himself as an electrical switchboard installer. As the person answering the call was indeed expecting such an installation at a construction site, an appointment was agreed upon. At the end of the call, the fraudster asked the victim to confirm the appointment using Smart-ID, and the victim entered their PIN1. This was followed by calls from fraudsters posing as a police officer and a bank employee, claiming that the victim's bank account had been accessed illegally and several transactions had been made. To reverse these, the victim was repeatedly asked to enter PIN1 and PIN2 codes. As a result, more than 120,000 euros were transferred from the non-profit organisation's account to the fraudsters.

A similar scheme was attempted against a Latvian project manager of the Äripäev newspaper. In the first call, the victim was asked to confirm the replacement of an electricity meter by entering a Mobile-ID code. This was followed by a call from a person posing as a bank employee, who claimed that an unknown individual had attempted to access the victim's bank account. A third call came from a fraudster posing as a police officer via WhatsApp, allegedly because the channel was harder to intercept. At some point, the calls began to seem suspicious, and the victim contacted their bank's account manager, who confirmed that it was a scam.

A MILLION-EURO FRAUD CASE GOES TO COURT

In August, it became public that the machinery manufacturer Hekotek had lost hundreds of thousands of euros to fraudsters. The chain of events began with a phone call to the company's chief financial officer, during which the callers posed as employees of the Estonian Health Insurance Fund. Using information obtained during that call, the fraudsters were able to create a new Smart-ID account in the CFO's name. Subsequent calls involved impersonating bank employees and police officers, allowing the fraudsters to access the CFO's computer via the remote desktop tool AnyDesk. They opened the banking application and authorised payments using the Smart-ID account they had created. Within two hours, 52 transfers were made from the company's account, totalling 1.6 million euros. Part of the money was recovered, but final losses still exceed one million euros. The company is now in a legal dispute with its former CFO, with the court expected to determine who bears responsibility for the damage and to what extent.

HOW TO RECOGNISE AND AVOID PHONE SCAMS

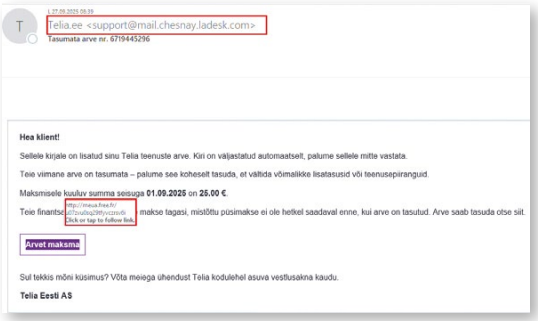
- Common phone scam schemes include:
  - warnings about suspicious transactions on a bank account
  - contact regarding supposedly unused compensation payments
  - requests for money to resolve an accident involving a relative, such as paying hospital bills
  - offers of attractive investment opportunities
- If you receive a call from an unfamiliar number with a foreign country code, do not answer it unless you are expecting such a call.
- Do not share personal information over the phone or enter it on websites to which you are directed during a call.
- Never share or enter your PIN codes. No bank or public authority will ask for them. A bank may request PIN1 to verify your identity only if you initiated the call yourself.
- Do not agree to move the conversation to an alternative communication channel, such as WhatsApp.
- If you are asked to install software, such as AnyDesk, on your device, end the call and do not install the software.
- If the caller pressures you to act quickly or uses fear tactics, take time and discuss the call with someone you trust.

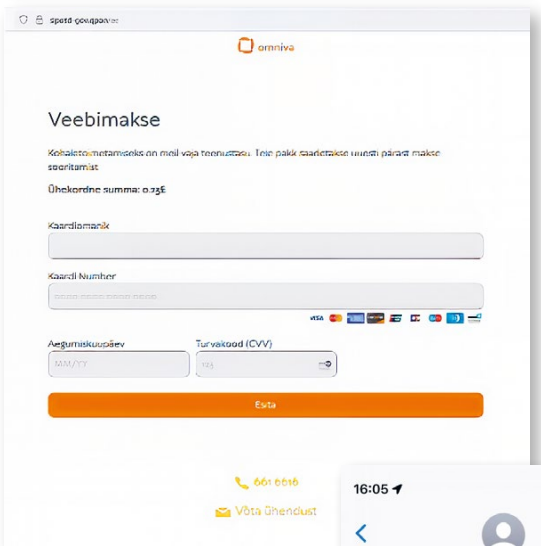
→

PHISHING CAMPAIGNS CONTINUED

In 2025, scam emails purporting to be from telecom providers Telia and Elisa circulated widely. These messages claimed that the recipient had either an unpaid invoice or a credit balance. In both cases, the email included a link that directed users to enter their bank card details. The messages were sent from suspicious email addresses that did not belong to the service providers in question. Neither company sends such emails or requests bank card or other sensitive details by email. All billing-related information is available through the companies' self-service portals.

Phishing messages impersonating postal and delivery service providers, familiar from previous years, also continued to circulate. These were sent both by email and via text message. Recipients were led to believe that a parcel was waiting for them and that, to receive it, they needed to pay customs charges or provide their bank card details under some other pretext. Such scams aim to obtain the victim's card details and use these to drain the account. Typically, the message suggests that only a few euros need to be paid, but the actual loss can be as high as the account balance or credit limit allows.





THE SUSPICIOUS LINKS AND SENDER DETAILS INDICATE A SCAM:
In such cases, pay close attention to the actual sender address, not just the displayed name, and to the domain used in any links. Check whether it genuinely belongs to the service provider named in the message. As a reminder, no institution – whether a bank, the police or a postal company – will ask for bank card details by email. Requests of this kind are a clear sign of phishing.

HOW TO AVOID FALLING VICTIM TO BUSINESS FRAUD

- Establish clear rules and procedures for processing payments within your organisation. For example, a two-person approval rule can be implemented, requiring that at least two employees confirm every invoice.
- Train employees regularly on cyber threats. This should include reminders on how to recognise phishing emails. One option is to use RIA's cyber test (www.kybertest.ee).
- Make it as difficult as possible for criminals to spoof your organisation's email addresses by configuring SPF, DKIM and DMARC.
- Protect email addresses published on your website from spam bots or, where possible, avoid publishing the email addresses of all employees.
- If in doubt, contact the supplier or business partner directly to verify the message. Always use a known contact number, not one provided in a suspicious email.

CEO FRAUD AND INVOICE SCAMS

CEO fraud involves an email that appears to come from a company's chief executive and is sent to an employee, often the chief financial officer or an accountant, requesting an urgent transfer. The real beneficiary of the payment is the fraudster. Invoice fraud, by contrast, involves sending an organisation a fake invoice in the name of a legitimate business partner.

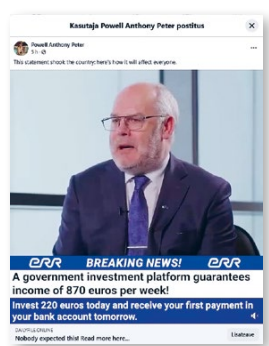
In August, an employee at one Estonian company was persuaded to purchase gift cards. The fraudster sent an email in the CEO's name and then

moved the conversation to WhatsApp. There, the employee was led to believe that the manager was requesting the purchase of gift cards. The employee complied and fell victim to the scam, resulting in total losses of approximately 550 euros.

In November, fraudsters carried out another successful invoice scam. A company received an email, apparently from a long-standing supplier, that attached an invoice and stated the supplier's bank account details had changed. As changes to banking details had occurred before, the invoice did not raise suspicion. The company paid the invoice for approximately 50,000 euros. It later emerged that the money had been transferred to the fraudsters' account and could not be recovered.

Also in November, details of a CEO fraud scheme carried out in 2022 at the Estonian Traditional Music Centre, a non-profit organisation that organises the popular Viljandi Folk Music Festival, became public. An email purporting to be from the organisation's director was sent to the accountant, asking about the account balance and requesting a 28,000-euro transfer. The accountant approved and made the transfer. The following day, another email requested a further transfer of 19,500 euros. A few days later, a third payment of 25,350 euros was made. All payments were sent to foreign bank accounts, and the emails instructing the payments appeared to have been sent by the centre's director. Once the fraud was discovered, one transfer could be cancelled, but total losses still exceeded 53,000 euros.

INVESTMENT SCAMS: LOSSES GUARANTEED



In 2025, people in Estonia lost nearly 6 million euros to various investment scams. Victims are presented with seemingly attractive investment opportunities, often advertised as low-risk or risk-free, with guaranteed high returns.

The proposed investments may include cryptocurrencies, shares or bonds that fraudsters promote as new products, technologies or business opportunities. Victims are contacted by phone, email, or social media and directed to a website that appears legitimate. Today, scam websites are highly convincing, and users may not realise they are being deceived when entering their personal details.

Not everything that glitters is gold. Unfortunately, the old adage applies here as well: if something seems too good to be true, it is very likely a scam.

Fraudsters are becoming increasingly sophisticated. Last year, for example, a video circulated in which President Alar Karis appeared to encourage people to invest in a new state-run platform. The video promised a guaranteed weekly income of 870 euros. It was, of course, a scam, and the video itself was a deepfake. The fraudsters sought to build credibility by exploiting the authority of the President of Estonia.

INVESTMENTS THAT ENDED BADLY

- During online communication, a 41-year-old woman was persuaded to make deposits on a cryptocurrency investment platform and to take out a loan to do so. She was unable to withdraw money from the platform and was repeatedly asked to make additional payments. The damage amounted to 9,936 euros.
- In the summer, a 68-year-old woman found an online advertisement for an investment opportunity and left her contact details on the website. Shortly afterwards, she was contacted by a person who presented themselves as an investment broker and guided her through the transfer process. The platform turned out to be fake, the money could not be recovered, and the supposed financial adviser disappeared. The loss was nearly 15,000 euros.
- A 39-year-old man saw an investment advertisement on Facebook and joined a WhatsApp group where the platform was explained and an account was created for him. With the help of a person posing as a broker, he made transfers and granted remote access to his computer via AnyDesk. He also took out several loans to invest more. The platform was fraudulent, and the money could not be recovered. The loss exceeded 28,000 euros.
- A 57-year-old man was contacted by someone presenting themselves as an investment adviser. Acting on the adviser's guidance, he registered on a cryptocurrency trading platform and made an initial deposit of 1,300 euros. Over the following six months, and in line with the fraudsters' instructions, he transferred 504,400 euros from his company's accounts to the fake platform.

ANOTHER RECORD NUMBER of vulnerabilities

More than 48,000 vulnerabilities were reported in 2025, an increase of around 20% from 2024. Serious vulnerabilities were found in network devices, industrial automation systems, operating systems and a wide range of other software.

The year stood out for the number of severe zero-day vulnerabilities, in which attackers compromised systems before the vulnerabilities were publicly disclosed and retained access even after patches were applied. Attackers also continued to exploit vulnerabilities known for years that remained unpatched. Increasingly, and with greater specificity, attention has focused on state-backed groups that search for and exploit vulnerabilities in critical infrastructure systems.

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 devices and software that have reached the end of their supported life and no longer receive security updates from the manufacturer.
- Protect your network and administrative interfaces. Use VPNs and restrict access to devices, especially system management interfaces, to specified IP addresses only.
- Configure and monitor system logs and deploy monitoring tools so that anomalies are detected, and incidents can be addressed quickly.

VULNERABILITY OF THE YEAR: REACT2SHELL

The most serious and wide-reaching vulnerability discovered in 2025 was the flaw disclosed in early December, which became known as React2Shell (CVE-2025-55182).

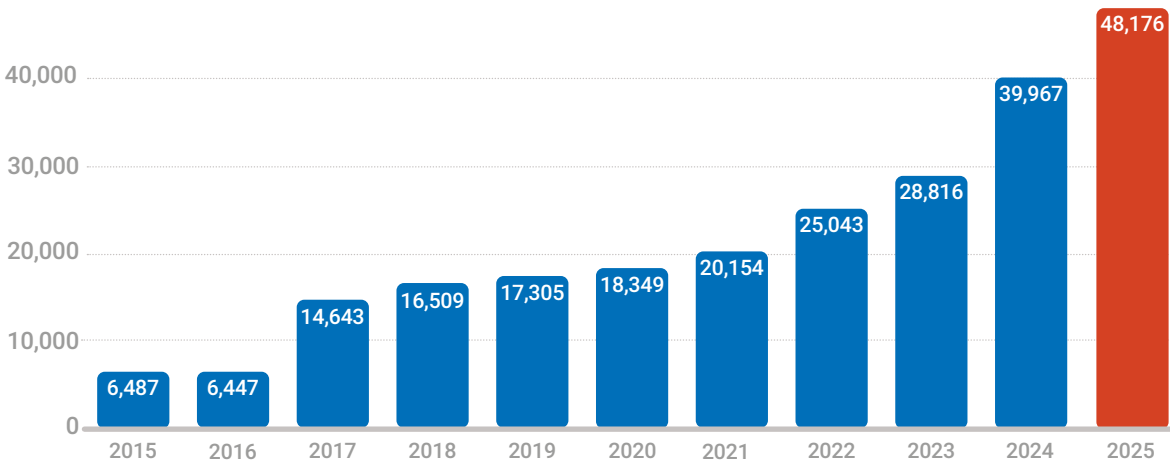
This remote code execution vulnerability affects React Server Components and allows an attacker to gain control of a vulnerable server with relative ease. Its impact is exceptionally broad because React is widely used on web servers, including web services, administrative panels and application programming interfaces (APIs). Several groups began targeting servers vulnerable to React2Shell within hours of its disclosure.

NETWORK DEVICES UNDER FIRE IN ESTONIA

Last year saw the discovery of zero-day vulnerabilities in several network devices, alongside attacks exploiting older, unpatched flaws. Users of FortiGate, Cisco and Ivanti devices all experienced unwelcome tension as a result.

At the beginning of the year, it emerged that VPN devices using Ivanti Connect Secure software at

NUMBER OF REPORTED VULNERABILITIES 2015–2025



SOURCE: NVD.NIST.GOV

two Estonian state authorities had been compromised. The attackers most likely exploited zero-day vulnerabilities (CVE-2025-0282 and CVE-2025-0283), compromising the devices before security updates were released. Later in the year, a new zero-day vulnerability (CVE-2025-20393) affecting Cisco network devices was found in Estonia.

In spring, malware was distributed through the systems of an Estonian library. Analysis of the incident showed that attackers gained access because security vulnerabilities in both the email server and the web content management software had not been patched, and the products had long reached the end of their supported life.

Several websites using WordPress were compromised. At Laagri School, for example, the new school year began with the compromise of the school's website: shortly after midnight, a script was launched via outdated WordPress software, blocking access to the site. The homepage displayed a login window requesting a username and password.

RANSOMWARE ATTACK EXPLOITING AN UNPATCHED VULNERABILITY

In autumn, an employee at an Estonian company discovered that a server had been encrypted, and a ransom demand was displayed on the screen. Analysis revealed that the attackers had gained access by exploiting a vulnerability that had been patched in August 2024. Unfortunately, the company had failed to install the relevant security update in time. As a result, attackers gained access to the system in spring 2025 and deployed ransomware in autumn.

THE EUROPEAN UNION VULNERABILITY DATABASE LAUNCHED

On 25 May, the European Union Vulnerability Database (EUVD) was launched and made public. The database is managed by the European Union Agency for Cybersecurity (ENISA). It aims to consolidate information relevant from an EU perspective on vulnerabilities, their impact, exploitation and mitigation measures.

In 2025, questions arose over the funding and long-term continuity of the Common Vulnerabilities and Exposures (CVE) system's vulnerability databases – cve.org and the National Vulnerability Database (NVD), managed by the US National Institute of Standards and Technology (NIST). As of year-end, the CVE system and its databases remained operational, but the EUVD can serve as an alternative if needed.

The global cyber landscape in 2025

Ransomware attacks battered the reputations of well-known brands, North Koreans using fake identities attempted to infiltrate international technology companies, and large-scale service outages exposed critical dependencies.

Ransomware is among the most damaging forms of cyberattack. It can bring large corporations or hospitals to a standstill, shut down pipelines, and cause damage measured in billions of euros.

In 2025, global efforts to reduce the impact of ransomware attacks and expose the criminal networks behind them continued. While the number of ransomware attacks worldwide increased, average profitability per attack declined.

OBLIGATION TO REPORT RANSOM PAYMENTS

In 2025, Australia became the first country to require certain sectors to report their decisions to pay ransom demands in the event of a ransomware attack. The reporting requirement aims to give the state a clearer picture of the scale and impact of ransomware attacks. It is also likely intended to encourage companies subject to the obligation to refrain from paying ransoms.

So far, Australia's approach remains the exception, but many countries follow an unwritten rule of not paying ransoms in cases where the public sector is targeted. Reports from several cybersecurity providers suggest that private companies are also increasingly reluctant to negotiate with criminals and pay ransoms. This indicates growing maturity in addressing cyber crises.

The number of ransomware attacks worldwide is nevertheless on the rise. While the impact of ransomware attacks often goes unnoticed by the general public, an attack in September against Collins Aerospace's check-in and boarding software caused chaos at several major European airports. Airlines were forced to check in passengers and luggage manually, resulting in long queues, missed connecting flights, and the cancellation of dozens of flights.

In September, a ransomware attack also disrupted operations at Asahi, one of the world's largest beverage producers, headquartered in Japan and best known for its beer. The attack was claimed by the Qilin ransomware group, which had attacked the South Korean conglomerate SK Group a few months earlier.

In the United Kingdom, several prestigious retail chains were targeted by attacks last year, including Marks & Spencer, Harrods, and Co-op. Marks & Spencer incurred the most significant financial loss, estimated at approximately 300 million

pounds, following a disruption to its online sales for several weeks. In France, cyberattacks targeted luxury brands Cartier and Dior.

The British car manufacturer Jaguar Land Rover suffered a severe economic and reputational blow after a cyberattack forced it to halt production for five weeks at several plants in the UK and abroad. The company also faced difficulties in delivering finished vehicles and spare parts, and attackers stole sensitive data from its systems.

The attack was claimed by the group Scattered Lapsus$ Hunters, but the company has not disclosed the perpetrators or detailed information. The attack on Jaguar Land Rover is estimated to have cost the UK economy approximately 1.9 billion pounds, making it the most costly cyberattack in the country's history.

SUPPLY CHAIN ATTACKS CONTINUED

In 2025, the trend of compromised supply chains and critical service providers persisted, significantly widening the cross-border impact of attacks. In August, criminals successfully attacked Salesforce, a customer relationship management platform widely used in the United States and elsewhere, and stole sensitive data from hundreds of companies and organisations that use the software. Victims included several international corporations, such as Google, Toyota, FedEx, Qantas and Allianz Life.

In attacks of this kind, criminals typically extract as much data as possible and then attempt to extort ransoms from the affected organisations one by one. The breach did not occur through Salesforce's core platform but exploited a vulnerability in Salesloft Drift, a marketing tool integrated with it. Attackers continually search for weak links in large systems, whose management, protection and interdependencies are becoming increasingly complex for businesses and public institutions alike.

SERVICE OUTAGES FELT AROUND THE WORLD

Triggering a domino effect that disrupts the operations of hundreds of organisations and companies does not always require attackers. On 20 October, digital services at more than a thousand companies were disrupted across several parts of the world. ➜

The incident originated in an Amazon Web Services (AWS) data centre in Northern Virginia, and subsequent analysis showed that the root cause was a failure in the Domain Name System (DNS) management service.

For up to 14 hours, the outage affected banks, airlines, entertainment platforms and logistics companies, impacting millions of people. The resulting damage is estimated in the billions of dollars. Some services used in Estonia, including the Signal messaging app, were also briefly affected.

Just a month later, on 18 November, another high-impact service disruption caused frustration worldwide. Due to a technical failure, network services operated by the global technology company Cloudflare were disrupted, with knock-on effects in Estonia as well. For a couple of hours, news portals such as Delfi, Eesti Ekspress and Õhtuleht were unavailable, and users were temporarily unable to purchase bus and train tickets via the Lux Express and Elron websites. According to a Cloudflare blog post, the outage was caused by an error during a routine database update, which triggered a cascade of technical failures affecting a large portion of the internet.

Three weeks later, on 5 December, Cloudflare experienced another service disruption, lasting approximately 20 minutes. It was caused by an internal configuration change the company had made to its firewall. The change was necessary to protect customers against the exploitation of a newly discovered critical vulnerability, but parts of Cloudflare's infrastructure were unable to handle it.

Even the largest operators encounter such incidents, yet we are not accustomed to recognising how dependent everyday life has become on a small number of global service providers.

STATE-BACKED GROUPS AND HACKTIVISTS

In our previous annual reviews, we have noted that geopolitical tensions shape cyberspace and that several states use highly capable hacker groups to pursue their strategic objectives. Such activity is usually covert, and the success of these groups depends on how well they can conceal their tracks and remain undetected in networks for extended periods.

When an attack is uncovered, the targeted state may choose to keep it confidential or, conversely, to attribute it publicly, often accompanied by sanctions or other legal measures. In 2025, several such cases made the headlines.

MANY STATE-BACKED ATTACKS ATTRIBUTED TO RUSSIA

January	The EU added three members of Russia's military intelligence Unit 29155 to its sanctions list, citing cyberattacks carried out against Estonia since 2020. Estonia had publicly attributed the attacks earlier, in September 2024.
April	France has attributed several past cyberattacks to the group APT28, which is linked to Russian military intelligence. These included the theft and leaking of emails from Emmanuel Macron's campaign team ahead of the 2017 presidential election, as well as infiltration attempts targeting organisations involved in organising the 2024 Paris Olympic Games.
May	The Czech government announced that it had identified links between the Chinese state-backed group APT31 and cyberattacks against the Czech Ministry of Foreign Affairs. The attacks began in 2022, when the Czech Republic held the presidency of the Council of the European Union.
December	The UK government imposed sanctions on Russia's military intelligence service, the GRU, in its entirety and on eight cyber intelligence officers by name. The measures were linked to the attempted poisoning of former Russian double agent Sergei Skripal in Salisbury in 2018 and to earlier cyberattacks against the phone of his daughter, Yulia Skripal, carried out for intelligence purposes.
December	The UK government also sanctioned two Chinese technology companies, known as i-Soon and Integrity Tech, for organising and supporting cyberattacks in the United Kingdom and other countries.

While public attribution tends to complicate the work of most state-backed threat actors, ideologically motivated hacktivists thrive on attention. They aim to create confusion, fear and public discontent, and they often seek to amplify the perceived impact of their attacks through media coverage. In 2025, hacktivist denial-of-service attacks against government websites and other critical sectors continued in several countries, but their overall impact remained limited. For greater effect and visibility, some hacktivist groups experimented with the manipulation of industrial control systems. In August, Norway's security service attributed an attack on the control systems of a dam regulating water flow in south-western Norway to pro-Russian hackers. Fortunately, no significant damage was done.

On 29 October, Canada's cybersecurity centre published a threat assessment describing successful hacktivist attempts to manipulate pressure equipment at a regional water facility and to alter the temperature and humidity levels of a grain drying silo on a Canadian farm.

In mid-December, Denmark's intelligence service revealed that a Russian hacktivist group had carried out a cyberattack against a local water utility at the end of 2024. As a result of the attack, 50 households were left without water for several hours.

In December, the US Cybersecurity and Infrastructure Security Agency (CISA) also warned that pro-Russian hacktivists were conducting opportunistic attacks against critical infrastructure in the United States and other countries. Although the growing frequency of such attacks is a cause for concern, hacktivist capabilities remain relatively unsophisticated, and cybersecurity measures applied to industrial systems have so far helped prevent more serious incidents.

AI IN THE SERVICE OF ATTACKERS

Both state-backed groups and cybercriminals are increasingly using AI tools to enhance and scale their activities, with social manipulation playing a growing role across many types of attack.

The scheme known as the North Korean IT worker fraud expanded its reach last year. Using AI-generated video and image material and fake identities, hundreds of impostors attempted to secure jobs at global companies. The scheme also operated in reverse: North Korean threat actors posed as employers on platforms such as LinkedIn and approached developers in other countries with fictitious job offers. The test assignments they sent as part of the recruitment process contained embedded malware.

The objectives of the North Korean scheme vary. They include stealing internal information from technology companies, infecting systems with malware for later extortion, or securing employment in Western companies in order to generate income for the benefit of the North Korean state.

In July 2025, a US citizen who had assisted the scheme was sentenced to nine years in prison. She had helped North Koreans obtain jobs at US companies using stolen identities.

According to Google's analysis, North Korean IT workers also targeted several European defence industry companies last year, with one individual using at least 12 different fake identities. Recruiters at some international companies operating in Estonia have also reportedly encountered the scheme.

As if hiring IT staff were not challenging enough already, there is now the added risk that offering remote work to a candidate with an impeccable CV and a convincing video interview may inadvertently support North Korea's nuclear programme.

DO NOT FEED THE CRIMINAL

For years, the business model of cybercrime has shifted toward greater specialisation. Different stages of an attack – from target selection and initial access to malware deployment and ransom demands – can be purchased as a service under the so-called ransomware-as-a-service (RaaS) model. To undermine the profitability of this criminal business, governments are seeking to reduce the likelihood that ransoms will be paid.

Rapid advances in AI tools create new opportunities for all actors, while also increasing unpredictability.

CYBERSPACE BECOMES MORE UNPREDICTABLE

In summary, 2025 saw the continuation of several established trends in the global cyber landscape: large-scale attacks carried out via service providers, ransomware attacks that disrupted everyday life and involved data theft and extortion, and the growing use of social manipulation to facilitate cyberattacks.

Outages triggered by a handful of technical errors disrupted people's lives in places as distant as Valga County and California, underscoring that even the most capable operators cannot eliminate disruptions entirely.

In a geopolitically tense world, state-backed cyber threat actors remain active. At the same time, both targeted states and companies that analyse cyber threats have become more willing to publicly expose such activity. Rapid advances in AI tools create new opportunities for all actors, while also increasing unpredictability.

War in Ukraine's cyberspace: THE DEFENCE HOLDS

Despite being Europe's most heavily targeted country by state-backed threat actors, Ukraine experienced no cyberattacks with a major societal impact in 2025, making it the first such year since the start of Russia's full-scale invasion.

In 2025, continued attacks on the public sector and critical infrastructure shaped Ukraine's cyberspace, as the aggressor sought to advance its war objectives and erode Ukrainian morale.

According to Microsoft's Digital Defense Report 2025, Ukraine was the most targeted country in Europe by state-backed threat actors. When conventional cybercrime is also taken into account, the same report ranks Ukraine fifth globally in terms of the intensity of cyberattacks.

The most common types of incident changed little: phishing, the distribution of malware for various purposes, malware infections, and the compromise of accounts and information systems all remained prevalent.

INTEREST IN SIGNAL MESSAGES

Cyberattacks and attempted intrusions are part of everyday life in Ukraine, as they are elsewhere, and threat actors seek to exploit both technological developments and user habits. In February, threat analysts at Google reported growing activity by Russian state-backed actors targeting the Signal messaging app, aiming to gain access to the accounts of individuals of interest and collect valuable intelligence.

In many cases, attackers abused Signal's feature that allows a single account to be linked to multiple devices. Linking a device requires the user to scan a QR code; if attackers succeeded in tricking victims into scanning a QR code they had generated themselves, the entire message history would then be synchronised to a device under their control. To create a convincing pretext for scanning the code, attackers forged Signal's own instructions or imitated applications used within the Ukrainian armed forces.

In late June, Ukraine's CERT-UA disclosed a second wave of attacks in which malware-laden documents were sent to government officials via messaging apps. Once again, these were precisely targeted attacks built around carefully constructed and highly credible contexts.

ARTIFICIAL INTELLIGENCE IN THE HANDS OF ATTACKERS

A broader global trend in 2025 was the use of artificial intelligence (AI) to enhance the effectiveness of cyberattacks, and this was also evident in Ukraine. Experts assess that AI tools were used both to make phishing attempts more convincing and to assist in writing malware code. Traces of

AI-generated code have been identified, for example, in malware known as Wrecksteel, which was used in attacks against Ukrainian government bodies and critical infrastructure. Wrecksteel's purpose was to locate sensitive files on a network and exfiltrate them to a server under the attackers' control.

A HARDENED DEFENCE

Years of operating under sustained attention from attackers of varying backgrounds – and, in some respects, serving as a testing ground for Russian groups – have hardened Ukraine's cyber defenders and gradually increased the country's cyber resilience. As noted, 2025 was the first year since the start of Russia's full-scale invasion in which Ukraine did not suffer a cyberattack with a major societal impact.

Ukraine experienced no cyberattacks with a major societal impact in 2025.

ATTACKS ON CRITICAL INFRASTRUCTURE

Attacks against critical infrastructure continued. In March, a cyberattack hit Ukraine's state-owned railway operator, Ukrzaliznytsia, disrupting ticket sales on its website and mobile app for several days. Long queues formed at ticket offices in major stations, although train operations and timetables were not affected. Ukrzaliznytsia is one of the world's largest passenger and freight rail companies and plays a vital role in the war effort, including in the evacuation of civilians.

The situation in cyberspace remains fluid, however. Because serious attacks typically require lengthy and well-concealed preparation, no far-reaching conclusions should be drawn from a single year of relative success. Estonia, like other countries, should therefore closely follow developments in Ukraine's cyberspace, as similar attack methods and patterns may appear elsewhere as part of Russia's broader hybrid campaign against the West. ●

HEAD OF SSSCIP: a peace deal won't bring peace to cyberspace

Brigadier General **OLEKSANDR POTII**, the head of Ukraine's State Service of Special Communications and Information Protection (SSSCIP), discusses events in Ukraine's cyberspace over the past year and the lessons others can learn from them.

How would you characterise the cyberattacks against Ukraine in 2025? What has changed compared to the previous year?

We observed a shift in the adversary's focus toward cyber intelligence, particularly espionage targeting the military and defence-industrial sectors. New threats have emerged in the cyber arena, and Russia is actively recruiting additional forces for attacks, often compensating for a lack of quality with quantity. In the past year alone, we have begun tracking about 20 new clusters of cyber threats.

An additional factor in this rapid development is the spread of artificial intelligence technologies. While in 2024 it was mainly used to generate phishing messages, in 2025, we saw not only malware created with the help of artificial intelligence, but also malware that internally uses AI algorithms to carry out malicious actions.

The number of destructive attacks has not decreased either. At the same time, they have become less noticeable, as a significant portion of such cyberattacks was neutralised in the early stages, which reduced their public resonance.

Have you seen any novel tactics by the nation-state threat actors in cyberspace? Are there any significant new threat groups that have emerged?

As mentioned earlier, we began tracking about 20 new cyber threat clusters in 2025. At the same time, known hacker groups, including state-sponsored ones, have not disappeared and continue to evolve. The development of protective measures forces attackers to change their approaches, which in turn leads to further improvements in protection. This is a continuous cycle of mutual adaptation.

The hackers' "cyber arsenal" is constantly expanded with new malware samples, including those that use advanced technologies. One example is the LAMEHUG malware used by the Russian GRU (UAC-0001, also known as APT28).

Today, malware distribution is no longer just a phishing email with an attachment, but often a complex social engineering operation that can last several days. At the same time, attackers have been actively using zero-click vulnerabilities as an alternative attack vector.

Overall, the last year was characterised by the active adaptation and development of hacker tactics, techniques, and procedures.

In December 2024, Ukraine experienced a cyberattack that affected several government databases. As a result, for a few weeks, people were unable to sell cars, file legal claims or

Brigadier General Oleksandr Potii, the head of Ukraine's State Service of Special Communications and Information Protection (SSSCIP)

register marriages digitally. Is there any lesson learned from this attack that you would like to share with Estonia?

Even the most advanced cybersecurity measures cannot guarantee 100% security – any organisation can become a target of attack at any time. That is why it is critically important to be prepared for the worst-case scenario, and backups must be stored in an isolated environment, separate from production systems. That remains the key to fast and controlled recovery.

What are some success stories from last year regarding thwarting cyberattacks against critical infrastructure?

Reducing the number of cyberattacks that achieve their goals is in itself an indicator of success. We focus on efficiency, particularly the exchange of actionable information about cyber threats in real time or as close to it as possible.

For example, in February 2025, we detected a cyberattack conducted by the Sandworm group. The primary method of infiltration was the distribution of emails with malicious attachments. Our analysis of this campaign revealed similar activity directed against more than 20 logistics companies and 25 developers of automated process control systems in Ukraine, as well as organisations in other European countries. This allowed us to respond quickly and prevent the attack from succeeding. Combining this exchange with the experience and high qualifications of local specialists who clearly understand how to respond to such signals enables the timely detection and neutralisation of attacks.

We are grateful to everyone who contributes to the exchange of information about cyber threats and shares their knowledge. We not only receive this data but also give back to the community our own experience and relevant information – because sharing is caring.

If 2026 should bring a ceasefire or peace agreement for Ukraine, what would the implications be in cyberspace? Do you think cyberattacks against your country would continue regardless? Or would Russia focus its attention elsewhere?

It is next to impossible to predict Russia's actions. Of course, we always hope for the best, but we are also preparing for any scenario. Even before the full-scale invasion, Russia carried out terrorist cyberattacks on Ukraine's energy infrastructure and continues to use cyberspace as a base for hybrid operations against Western countries, our partners, and anyone else they are interested in. Therefore, even if a peace agreement is signed, it is unlikely that attacks in cyberspace will stop completely. Their number may decrease, but they will not disappear.

From the outside, it appears that the last really destructive cyberattack in Ukraine was the one against Kyivstar in December 2023. Considering the ongoing warfare in Ukrainian cyberspace, do you think the worst is behind you, or is the worst yet to come?

We have survived more than one destructive cyberattack – Kyivstar in December 2023, state registries in December 2024, and Ukrainian Railways in March 2025. Our constant improvements to our cyber defence are probably why December 2025 was relatively calm. Does this mean that the worst is behind us? I don't think so – the enemy is constantly carrying out cyberattacks. Some of them are more successful, others less so. We are doing everything possible to prevent the worst, but if it does happen, we will be ready.

Cyber menu 2025: PEKING DUCK

Western countries are increasingly attributing cyberattacks to China and regard it as the biggest threat to their cybersecurity. Data leaks have given us a glimpse into China's offensive cyber ecosystem, which is characterised by extensive cooperation between the private sector and the state.

In the previous RIA cybersecurity annual review, we wrote that the cyber groups of the People's Republic of China are likely the most capable anti-Western forces in the world at conducting complex cyber operations. In 2025, we saw this trend intensify, with China's cyber activity expanding in reach and scale – from global espionage and attack campaigns to pre-positioning in Western critical infrastructure.

China's activity in cyberspace is characterised by advanced technical capabilities, rapid exploitation of vulnerabilities (including zero-day vulnerabilities), a global scope of operations, and support for China's national ambitions.

SWEET-AND-SOUR CHICKEN

In 2025, dozens of cyberattacks were attributed to state-backed attackers from China, known as advanced persistent threats (APTs). These groups mainly targeted government bodies, telecommunications companies and (defence) industrial firms, but companies in other sectors were also affected.

Their primary goal is to gain access to sensitive data to derive economic, political, and military advantage. In January, for example, Taiwan reported that Chinese attacks against the country had doubled, with government bodies and telecommunications firms hit in particular. In May, the United Kingdom's cybersecurity authority declared that it considered China the primary threat to national cybersecurity, as Chinese groups had targeted government bodies, critical infrastructure and members of parliament. Estonia's foreign ministry also condemned these attacks. According to the assessment of the US Director of National Intelligence, China is the most active and long-term cyber threat to the United States.

In May, the Czech Republic attributed an attack to the Chinese group APT31 for the first time, stating that the campaign had targeted the Czech foreign ministry. France's cybersecurity authority published a report on an attack campaign it calls Houken, which targeted France's government sector and private companies. These are only a few examples, but they illustrate the scale of China's state-backed cyberattack campaigns.

Reports of pre-positioning also continued. For example, the US Cyber Command discovered Chinese malware on the networks of several Latin American countries. The concept of pre-positioning

gained wider attention in 2024, when US authorities accused Chinese cyber groups of infiltrating various networks. The suspected aim is to position themselves so that, at a chosen moment, they can disable critical infrastructure and disrupt the day-to-day functioning of the targeted state and its population. The Salt Typhoon campaign, which received extensive coverage in 2024 and targeted the telecommunications sector, did not subside. On the contrary, it expanded: instead of the eight companies initially identified, more than 600 companies across 80 countries have now been targeted.

China also remains the biggest exploiter of zero-day vulnerabilities. In 2025, for example, Chinese cyber groups actively exploited vulnerabilities in Ivanti VPN devices in March, SAP NetWeaver in April, Ivanti Endpoint Manager in May and Microsoft SharePoint in July. The Microsoft SharePoint vulnerability was used to attack more than 400 organisations worldwide, including US government agencies. ➜

CHINESE CHOPSTICKS, OR 筷子

The modus operandi of Chinese cyber groups is to gain access to networks and remain undetected for as long as possible. They often attempt to move from one system to another by exploiting the fact that devices or systems already trust each other. In 2025, nearly 75% of the analysed Chinese cyberattacks were malware-free, meaning that attackers gained access either by exploiting vulnerabilities or by using stolen login credentials. This technique, known as Living off the Land (LotL), makes intrusion attempts harder to detect.

Another trend is the continued exploitation of vulnerabilities in edge devices and cloud platforms. This was also highlighted in a public advisory issued in September by the United States and its allies, with contributions from several dozen intelligence and cybersecurity agencies.

The European Union Agency for Cybersecurity (ENISA) notes in its annual report that a growing number of Internet of Things (IoT) devices, including routers, are being abused. The Chinese group Flax Typhoon exploited the Quad7 botnet, which consisted of thousands of TP-Link routers in Europe. Another example is botnet BADBOX 2.0. According to Google, it contained more than 10 million infected home devices that cybercriminals could use to carry out malicious activity. Estonia was not spared either – at the height of the campaign, more than 7,000 infected devices were identified in Estonia. In many cases, malware had been installed on devices before they were sold, or users infected their devices by downloading Android apps from unofficial sources. Most such devices originate from China.

The Chinese group Flax Typhoon exploited the Quad7 botnet, which consisted of thousands of TP-Link routers in Europe.

Another characteristic is that Chinese groups share tools with each other. This often makes it difficult to attribute a specific tool to a specific actor. For this reason, recent attributions have increasingly focused less on identifying a single group and more on naming Chinese companies that facilitate cyberattacks.

SPILLS IN THE KITCHEN

In November, more than 12,000 classified documents were leaked from the Chinese software company Knowsec. The leak revealed how the company compromised more than 80 targets worldwide. It also showed that Knowsec has malware and trojans

DEEPSEEK AND THE END OF THE ‘FREE LUNCH’

The United States and China are engaged in a technological race, with AI as its most visible front. At the start of 2025, the Chinese company DeepSeek surprised the public with a new large language model, which was reportedly developed at a fraction of the cost of Western equivalents. Yet it did not lag behind the Western language models of the time in capability. In the United States, DeepSeek’s announcement was described as a “Sputnik moment” in the AI field, as it became clear that China might not only catch up in AI development but also pull ahead.

The potential advantages of using DeepSeek’s language models are straightforward: they are powerful, relatively open, inexpensive, and fast, and can be used across applications, services, and businesses. DeepSeek’s own terms of use state that it collects data, uses it to train the model and shares it with other service providers. Under Chinese law, it must also share all data with China’s government and intelligence agencies. DeepSeek’s language models also censor topics that are uncomfortable for the Chinese Communist Party, such as the Tiananmen Square massacre in the summer of 1989.

None of this means that Chinese applications should always be avoided. It is important to remember, however, that there is no such thing as a free lunch. In government bodies and other critical organisations, RIA recommends that DeepSeek applications not be used on work devices. Sensitive information should not be entered into them either. Every user should think carefully about what information they share with technology companies.

for all major operating systems – Windows, Linux, macOS, iOS and Android.

A second leak contained personal data and transaction information relating to members of the Salt Typhoon group. A third described how China exports its internet model to other countries, enabling mass surveillance of citizens. A fourth leak revealed how Chinese companies use AI to run information operations in the political sphere.

These leaks show that the Chinese state relies on the help of private companies to conduct malicious cyber operations. At the same time, this gives the state room to distance itself from attacks, since the operator is a private company rather than a state body.

CHINESE FOOD IN ESTONIA

In 2025, Estonia also came within the scope of China's cyber activity. It is important to recognise that when a vulnerability is disclosed and actively exploited elsewhere, vulnerable devices are likely to be present in Estonia as well. It is only a matter of time before a malicious group finds them. To RIA's knowledge, several vulnerabilities that Chinese cyber groups actively exploit have also been tested in Estonia and, in some cases, successfully exploited.

We would like to remind readers that rapid patching and good cyber hygiene help prevent a significant proportion of cyber threats. Estonian companies are also being impersonated in SMS phishing campaigns created by Chinese cyber criminals, and we have been targeted by phishing emails from China's state-backed attackers as well.

'WHEN MANY GATHER FIREWOOD, THE FLAME WILL RISE HIGH' *

More and more Western countries are describing China as a cyber threat in increasingly explicit terms and attributing cyberattacks to it. Joint statements have been issued by the Czech Republic, the United Kingdom, France, the United States and others, and the tactics used by Chinese hackers have been described in detail. We should prepare for Chinese cyberattackers to increasingly use AI to identify and exploit vulnerabilities more quickly.

What can we do to counter cyber threats originating from China? Patch vulnerabilities faster, monitor what is happening in our networks, and strengthen domestic and international cooperation.

* a Chinese proverb

TWELVE YEARS OF CHINA'S STATE-BACKED CYBER GROUPS

In February 2013, the cybersecurity provider Mandiant published a report that shook the cyber world. It described a clandestine Chinese hacking group behind numerous espionage operations. The group was named APT1 and was linked to Unit 61398 of the People's Liberation Army.

The report described how the group stole hundreds of terabytes of data from nearly 150 organisations in more than 20 countries. It also named individuals who were behind the attacks. This was the first attribution of its kind, after which Western governments and companies began to speak much more openly about cyber threats. The issue became one of the main topics discussed by US and Chinese leaders in 2015. The two powers agreed that they would no longer engage in cyber-enabled intellectual property theft, and the pact became known as the Obama–Xi Cyber Agreement. Unfortunately, the agreement was short-lived.

Over the following 12 years, dozens of Chinese state-backed hacking groups were discovered. Analysts believe that China has the largest number of state-supported cyber groups. While it is difficult to give an exact number, there are thought to be at least 60. By comparison, the total number of groups linked to other major anti-Western cyber powers – such as Russia, Iran and North Korea – is believed to be fewer than 30.

In Chinese culture, time is traditionally measured in 12-year cycles. In 2025, 12 years after the first APT report was published, a new actor was added to the list of China's state-backed hacking groups: Phantom Taurus. While APT1-type groups had a broad scope and sought to collect as much data as possible, newer groups tend to carry out more targeted attacks, aiming to remain hidden within an organisation's or company's network for as long as possible. Phantom Taurus uses novel tools that have not previously been observed among Chinese groups. Notably, Phantom Taurus operated for two and a half years without being detected.

RUSSIAN BEARS in cyberspace

Russia employs cyberspace as a targeted and effective tool to further its foreign and security policy objectives. Its arsenal includes cyber espionage, destructive attacks and information operations.

To carry out such large-scale and coordinated cyber activity in practice, the Russian regime relies, among other things, on state-backed cyber groups, which are internationally known as APTs (advanced persistent threats). These groups can conduct complex and targeted cyber operations aimed at collecting intelligence, maintaining persistent access to compromised information systems and, where required, carrying out disruptive or destructive attacks.

They operate in the interests of Russian special services and military structures and perform intelligence-gathering and preparatory tasks both in peacetime and during a full-scale military conflict.

The activities of Russian APT groups are not limited to cyber operations against Ukraine. They also target countries that support Ukraine politically, economically or militarily. The European Union and NATO member states have remained persistent targets, with attacks aimed at collecting sensitive information and preparing the ground for potential influence or attack operations.

A NEW ARRIVAL: LAUNDRY BEAR

Alongside previously known and widely reported Russian APT groups such as Cozy Bear and Fancy Bear, which have targeted EU and NATO member states for years, a new and previously unknown Russian group emerged in 2025. Within the cybersecurity community, it became known as Laundry Bear (referred to by Microsoft as Void Blizzard).

According to assessments by the Dutch intelligence and security services (AIVD and MIVD), Laundry Bear is very likely a state-sponsored Russian group whose activities since 2024 have focused primarily on cyberattacks against Western countries. Its primary targets are government authorities, defence organisations, foreign ministries, defence industry companies, and other entities in EU and NATO member states that support Ukraine.

The nature of Laundry Bear's operations and its choice of targets point primarily to intelligence gathering rather than to disruptive or destructive cyber activity. Its main objective is to collect sensitive information, including email correspondence, contact details and other internal organisational data,

enabling Russian intelligence services to gain a clearer picture of Western political, military and defence-related intentions.

From a technical perspective, Laundry Bear is not characterised by the use of novel or particularly sophisticated attack vectors. On the contrary, the group relies on relatively simple but effective methods, such as abusing stolen user credentials, password spraying, exploiting authentication cookies (session cookies), and compromising cloud-based email environments, particularly Microsoft Exchange Online.

Any employee can become a target in organisations of interest to an attacker, regardless of their role or level of access.

The necessary authentication data are often obtained from third parties, using spyware-collected credentials sold on dark web marketplaces. This approach is illustrated by the 2024 attack against the Dutch police, in which Laundry Bear gained access to an employee account using a stolen login session. Through this access, the group collected work-related contact details and other information from central systems, which can be used to prepare further targeted attacks.

This case once again demonstrates that any employee can become a target in organisations of interest to an attacker, regardless of their role or level of access. However, it should be noted that most such attacks are easily preventable by following the basic principles of cyber hygiene, including multi-factor authentication, strong password management and user awareness training.

VENOMOUS BEAR AND COZY BEAR TARGET DIPLOMATS

Diplomatic targets have been a strategic priority for Russian state-backed cyber espionage for years, and 2025 brought no change in this regard. Foreign ministries, embassies and other diplomatic missions represent high-value intelligence targets for Russia, as they provide access to early information on political positions, decision-making processes, alliance relations and discussions related to Ukraine. In 2025, two long-established Russian APT groups stood out in this domain: APT29, also known as Cozy Bear, and Venomous Bear (also known as Turla).

APT29, which is linked to Russia's Foreign Intelligence Service (SVR), continued targeted phishing campaigns against employees of European diplomatic institutions. These attacks relied on credible and context-aware lures, with attackers posing as representatives of foreign ministries or similar bodies and sending apparently official email invitations or notifications, such as for diplomatic events or meetings.

The messages contained malicious links or attachments; if the target failed to exercise sufficient caution and interacted with them, attackers gained access to the victim's work computer and email account. This enabled APT29 to monitor communications, collect documents and use the compromised account to prepare further targeted intelligence operations.

Venomous Bear, considered one of Russia's longest-running and technically most capable APT groups and associated with the Federal Security Service (FSB), pursued a different approach in its continued operations against diplomatic targets in 2025. While APT29 primarily relied on phishing emails targeting EU diplomats abroad, Venomous Bear focused on diplomatic missions and staff based within Russia, using local communications and network infrastructure.

This allowed Venomous Bear to redirect diplomats' web traffic to an adversary-in-the-middle setup, where users were presented with a seemingly legitimate certificate error or security warning. To resolve the issue, victims were prompted to download and install a software component, which granted attackers access to the device and the ability to monitor diplomatic communications.

STEPS TOWARDS AUTONOMOUS MALWARE

Rapid advances in artificial intelligence (AI) and large language models (LLMs) in recent years have created new opportunities to automate and streamline everyday work tasks, but these technologies have also been widely applied to cybercrime.

They have enabled the automation and acceleration of the preparatory stages of cyberattacks, such

APT GROUPS LINKED TO RUSSIAN INTELLIGENCE SERVICES

	FANCY BEAR / APT28	COZY BEAR / APT29	VENOMOUS BEAR / Turla	LAUNDRY BEAR / Void Blizzard
Targets	Government authorities, defence industry, technology and logistics companies, critical infrastructure, and NATO- and EU-related international institutions	Primarily EU and US government authorities, non-governmental organisations, the energy sector, foreign and security policy institutions, and technology and cloud service providers	Government authorities in Eastern Europe and Southeast Asia, including foreign ministries, diplomatic missions and security agencies in Europe and Eurasia, as well as international organisations and research institutions	Government authorities in NATO member states, telecommunications companies, the healthcare sector, the defence industry, and the media and transport sectors
Affiliation	Russian military intelligence (GRU)	Russian Foreign Intelligence Service (SVR)	Russian Federal Security Service (FSB)	Unknown
Activity	Multiple intelligence campaigns against logistics and transport companies in Western countries supporting Ukraine in recent years	Continued intelligence campaigns against European diplomatic institutions using phishing emails containing malware	Intelligence campaigns against European diplomatic foreign services in the past year	Most recently linked to a cyber espionage incident targeting the Dutch police, during which the group gained unauthorised access to internal contact details

as crafting phishing messages, profiling targets, and tailoring attack scenarios to specific contexts and victims.

Among state-backed Russian threat actors, APT28, also known as Fancy Bear, is among the most notable users of these capabilities. This group, linked to Russian military intelligence, used its own custom malware in cyberattacks in 2025. The malware became known as LAMEHUG within the cybersecurity community.

According to several researchers, LAMEHUG represents the first publicly documented case of malware that directly uses an LLM in an attack operation. During an intrusion, LAMEHUG employs an LLM to generate specific malicious system commands and scripts, which the malware then executes on the infected system. These commands are used, among other things, to collect system information, search for user files, and aggregate and exfiltrate the collected data to the attacker. Unlike traditional malware, LAMEHUG does not rely on static code. Instead, it can appear in different forms and variations during an operation, leaving fewer recurring patterns and making detection by traditional antivirus and signature-based solutions more difficult.

LAMEHUG is not yet fully autonomous, decision-making AI-driven malware, but it illustrates how attackers use language models to apply existing attack tactics more flexibly and efficiently. These, however, are only the first steps. In the coming years, we are likely to see more autonomous malware capable of independently adapting its behaviour to the compromised system and deployed defences. Such developments would represent a qualitative leap in malware evolution and pose a significant challenge to existing detection and protection mechanisms.

THE MINISTRY'S PERSPECTIVE: developments and next steps

TÕNU GRÜNBERG, Deputy Secretary General for digital infrastructure and cybersecurity at the Ministry of Justice and Digital Affairs, looks back on developments in national cybersecurity over the past year and sets out priorities for 2026.

From the ministry's perspective, 2025 was a turning point in Estonia's cybersecurity evolution. Our focus was on ensuring that the digital state remains reliable, resilient and aligned with the rapidly evolving legal framework of the European Union. This involved both strategic frameworks and practical steps that help organisations better understand security requirements and put them into practice.

PRIMARY SECURITY MEASURES FOR SMALL ORGANISATIONS

One of the most significant steps was the introduction of a framework of primary security measures for small and micro-enterprises. The Estonian Information Security Standard (E-ITS) is a robust and comprehensive framework that establishes clear principles for cybersecurity management. Still, it is best suited to larger organisations with the capacity to assess and implement security requirements systematically. For smaller organisations, the situation is different. They often lack the expertise, time and human resources needed to navigate complex requirements independently or to assess where to start and which measures matter most for them.

Small and micro organisations primarily need clear, practical and unambiguous guidance – a concrete understanding of what they need to do to ensure an adequate level of cybersecurity that matches their size and resources.

It was precisely this need that led us to develop the framework of primary security measures. These help organisations focus on what is essential, reduce administrative burden and deliver tangible improvements in security. The practical value of the primary security measures framework was recognised by the Estonian Society of Family Doctors, who awarded it their "initiative of the year" distinction.

CYBERSECURITY LEGISLATION UPDATED

Another significant milestone was the amendment of the Estonian Cybersecurity Act, which entered into force at the beginning of 2026 and incorporated the EU's NIS2 Directive into Estonian law. Our work does not end with the adoption of the act. The next steps include implementing the relevant regulations and further reviewing several proposals with stakeholders.

To avoid over-regulation, we assessed each provision to determine whether it met or exceeded the

Tõnu Grünberg, Deputy Secretary General for Digital Infrastructure and Cybersecurity at the Ministry of Justice and Digital Affairs.

directive's minimum requirements. We used a simple but visually effective analytical approach to quickly identify the directive's mandatory requirements, specific obligations arising from existing national legislation, and potential risks of over-regulation, overly rigid rule-setting that limits flexibility, and outright non-compliance.

This approach gave decision-makers and stakeholders a clear overview of which elements strictly followed the EU framework and where Estonia was making deliberate national policy choices. It is a practice that should be applied more broadly in the incorporation of EU directives into national law and in legislative drafting generally. It enhances transparency, legal clarity, and trust throughout the process.

PREPARING FOR THE ARRIVAL OF QUANTUM COMPUTING

Another key focus has been tracking advances in quantum computing, which threaten to make today's cryptographic solutions obsolete and weaken the protection of data and services. In 2025, we began developing a roadmap for post-quantum cryptography. This provides clear guidance on preparing for the transition to new cryptographic algorithms as advances in quantum computing render existing solutions inadequate. The aim is to avoid rushed solutions and instead pursue a deliberate, well-timed transition that considers technological dependencies, priorities and organisational readiness.

MOVING INTO THE NEXT PHASE OF DEVELOPMENT

Looking ahead, we aim to move towards a more user-centred and effective system, supported by tools and capabilities designed to prevent incidents before they occur. Cybersecurity must be part of business operations and everyday life. This means that security requirements must become more user-friendly, so that they are easier to understand and implement, including for small organisations and for non-expert technology users.

One important new capability under development is a national cyber operations centre, which will enhance nationwide situational awareness, response capacity and cooperation in preventing and managing cyber incidents.

Looking ahead, we aim to move towards a more user-centred and effective system, supported by tools and capabilities designed to prevent incidents before they occur.

On the legislative front, 2026 will see the incorporation into national law, at the minimum necessary level, of the directly applicable EU Cyber Resilience Act (CRA) and the Cybersecurity Act (CSA). Our objective is to meet the requirements in a reasonable and proportionate manner, without an excessive administrative burden, while ensuring that safer digital products reach the market.

Overall, we are moving steadily into the next phase of the digital state's development, where the focus is not only on requirements and technology but also on clarity, cooperation and trust.

CERT-EE: 20 years of protecting Estonia's cyberspace

On 1 January 2026, CERT-EE marked its 20th anniversary. The occasion offers an opportunity to reflect on Estonia's eventful history of incident response to be better prepared moving forward.

CERT-EE (Computer Emergency Response Teams) forms one of the most critical defensive lines of its digital state. The team operates largely out of sight, seeking to provide solutions rather than attract attention. Its success is measured by how rarely the public needs to be informed about critical cyber incidents.

TWO PEOPLE FENDING OFF A CYBER CAMPAIGN

In the 2000s, internet use grew, and attack vectors expanded as more services moved online. While hackers, malware and phishing were not yet everyday terms in Estonia, banks were already facing their first cyberattacks, and various incidents sparked debate about how to secure an increasingly digital information society.

In 2005, Toomas Viira, then head of information security at RIA, was tasked with developing a vision for an Estonian CERT and explaining the need for such a unit to both civil servants and politicians. At a time when Estonia's digital state was rapidly developing but cybersecurity remained a new and abstract concept for many, Viira spent months answering basic questions about what a cyber incident is and why it requires attention at the state level. It soon became clear that Estonia could not afford digital solutions that were innovative but unprotected. After months of groundwork, a favourable decision followed.

CERT-EE began operations on 1 January 2006. "Even then, we were already seeing early, rudimentary forms of phishing and viruses. Banks and their customers were the primary targets, but several other organisations were also affected," Viira recalls. Although the start was far from smooth – with processes to be built and trust to be established – he notes that CERT-EE was created at the right moment, just ahead of the 2007 cyberattacks.

The unit's first head, Hillar Aarelaid, faced a baptism of fire. Following the removal of the Bronze Soldier monument in Tallinn, the world's first coordinated cyber campaign – also known as Cyber War I – unfolded, disrupting Estonian websites and services. CERT-EE coordinated the response with a team of just two people: Aarelaid and Tarmo Randel. Randel, who later became head of the unit, wrote in CERT-EE's annual summary that the spring of 2007 put Estonia on the global map and that, despite the negative nature of the events, the overall effect was positive. For the public, it was the first time a cyber incident was recognised as a national security issue, prompting many companies and states to seriously analyse and protect their infrastructure.

WHAT IS CERT-EE?

CERT-EE is RIA's incident response department that monitors Estonian cyberspace, provides preventive protection for the public sector and detects cyber incidents in Estonia's computer networks. When an incident occurs, CERT-EE helps identify its cause and advises on response and remediation.

CERT-EE is a member of the CSIRTs Network coordinated by the European Union Agency for Cybersecurity (ENISA).

THE HECTIC 2010s

During the 2010s, CERT-EE's workload grew explosively. While around 300 incidents were handled in 2013, the number had increased tenfold just four years later. Klaid Mägi, who led the unit between 2014 and 2018, likens the team at the time to a start-up: "It was a group of enthusiasts doing big things with whatever tools were available, often improvised."

By 2015, it became clear that a 9-to-5 model was insufficient for effective incident response. A round-the-clock duty system was introduced, additional experts were hired, and from the summer of that year, Estonia's cyberspace was monitored 24/7.

"Continuous rapid response made it possible to warn the public about major phishing and malware campaigns, notify hosting providers and website owners about compromised sites and share more timely information about vulnerabilities affecting large numbers of users," Mägi explains.

This period also saw the launch of CERT-EE's daily newsletter, which continues to provide up-to-the-minute overviews of developments in cyberspace. Today, it has nearly 2,200 subscribers.

READY FOR ANNIVERSARY ATTACKS

In 2017, CERT-EE achieved SIM3 (Security Incident Management Maturity Model) certification for the first time – the highest international standard for CERTs. Certification assesses documentation, readiness for cooperation, workflows, the effectiveness and professionalism of incident ➜

handling, and information sharing, among other aspects that underpin strong response capabilities and cybersecurity. CERT-EE was the fifth organisation globally to reach this level.

The same year, preparations were made for the tenth anniversary of the 2007 cyberattacks, amid expectations of possible repeat attacks from Russia. "We assumed that our neighbour might mark the 'anniversary' in some way, and we were ready. Fortunately, no such attacks came, but the year did bring two other high-profile incidents – WannaCry and NotPetya – both of which had a major global impact," Mägi recalls. As if that were not enough, the Estonian electronic ID card crisis followed later that summer, affecting around 750,000 people. Challenges were plentiful.

Amid these events, the team honed its technical analysis and strengthened its automated detection systems. CERT-EE experts appeared frequently in the media and on social platforms, emphasising the importance of cybersecurity.

To coordinate responses to major international cyber incidents, CERT-EE members established an international Mattermost channel – a secure, controlled communication platform – that connects CERTs across EU member states. This channel, which remains active today, was first used to jointly address the WannaCry crisis.

WE DO NOT SETTLE FOR YESTERDAY'S STANDARDS

Over two decades, CERT-EE has grown into a trusted and credible actor that protects Estonia's digital ecosystem – from individual citizens to the state's critical infrastructure. National information security capabilities have strengthened, but as strong and independent teams multiply, the role of a central coordinator becomes increasingly important. Cyber resilience does not emerge from isolated efforts but from well-organised cooperation.

"If CERT-EE has proven anything over the past 20 years, it is that Estonia's digital state endures because we do not settle for yesterday's standards," says CERT-EE's head, Taavi Kupper. "The team continues with the same sense of responsibility, commitment and purpose to ensure that Estonia's digital state remains trustworthy – not only today but also tomorrow."

THE THREAT LANDSCAPE BEGINS TO SHIFT

Although cyber threats were no longer a novelty by 2019, the frequency, automation and targeting of attacks against Estonia increased. That year also saw a sharp rise in phishing and fraud schemes linked to Smart-ID, Estonia's widely used digital authentication service. It became clear that awareness-raising alone was no longer sufficient, prompting CERT to change its approach. "Giving advice is easy. But if an organisation cannot implement it, it makes more sense to offer the solution as a service," recalls Tõnu Tammer, who was leading the unit at the time. CERT expanded its portfolio with practical, scalable services that help prevent threats even when organisations lack in-house capacity. One example was the development of a DNS-based solution to filter cyber threats, blocking malicious activity before a connection is even established.

Alongside these substantive developments, important steps were also taken to strengthen Estonia's internet infrastructure. The national internet exchange point was upgraded, enabling operators to exchange traffic more efficiently and keep domestic traffic within the country. This improved both service continuity and resistance to attacks.

RAISING ATTACKERS' COSTS AND CUTTING RETURNS

In 2022, a new phenomenon emerged: web links that, once opened, caused the user's browser to participate in denial-of-service attacks automatically. "All it took was opening a link, and even a technically unskilled person could unknowingly take part in an attack," Tammer explains. In response, Cloudflare's services were adopted, further strengthening Estonia's defences.

The aim was to raise attackers' costs and lower their returns. "The more we can achieve this through technical measures, the less incentive there is to attack Estonia," Tammer says.

Cooperation with security solution providers was further expanded, with CERT sharing validated threat intelligence. This enabled threats to be added to blocklists more quickly, narrowing attackers' room for manoeuvre. According to feedback from one major vendor, information shared by CERT-EE accounted for a significant portion of its initial threat intelligence.

Looking back on CERT-EE's development, Tammer notes that the organisation has become increasingly proactive: "The team keeps cyberspace functioning and reduces risks – often without anyone noticing."

This is the paradox of cyber defence: the better the work, the less visible it is. When users do not need to think about service instability or outages, it means CERT-EE has done its job well.

EVERY DAY, ALL THE TIME

Driven by geopolitical developments, CERT's workload grew markedly in the following years. Veikko Raasuke, who has led the team since 2023, describes the work as a daily struggle. "We are attacked every day, attempting to break into systems or bring services down through denial-of-service attacks. CERT-EE's task is to push back at all times – on weekends, at night, during school holidays, public holidays and Christmas. In other words, when most of us are with our families, cyber guards are at work so the rest of the country can enjoy their festive meals," Raasuke says.

On 9 March 2024, Estonia experienced the most significant denial-of-service attack in its history against public-sector websites: in just over four hours, nearly three billion malicious requests were recorded. CERT-EE has been, and remains, effective in defence. Attacks rarely have an impact, and when they do, it is usually short-lived.

As CERT-EE continuously develops its defensive tactics, adversaries refine their tools and adjust their attack methods. According to Raasuke, denial-of-service attacks dominated the workload, alongside various phishing campaigns. In one case, criminals exploited a major international event held in Estonia and attended by senior officials from many countries. They sent participants a highly convincing phishing email purporting to come from the organisers.

Where it once took CERT-EE seven to ten working days to shut down a fraudulent financial website, cooperation with the Estonian Police and Border Guard Board, as well as the Banking Association and individual banks, reduced this to under an hour.

The team jokingly refers to the period from October to January as "Christmas peace", a tongue-in-cheek label for a time when fraud posing as logistics companies surges dozens of times. Usually, activity subsides after the holiday season. In January 2024, however, the lull never came. Fraudsters became even more active, expanding beyond logistics firms to target a wide range of companies and public authorities. "Here, too, the development of AI has been a major enabler, helping fraudsters easily produce credible Estonian-language content," Raasuke notes.

LOOKING AHEAD

Turning from the past to the future, CERT-EE faces increasingly complex challenges. Cybersecurity is no longer a concern for individual organisations alone, but a global issue. Entirely new threats are emerging, including AI-enabled attacks, the potential of quantum computing and vulnerabilities associated with 5G networks.

Taavi Kupper, who currently heads the unit, says that while Estonia's information systems and e-services are highly secure, the environment is constantly changing. "New threats require continuous adaptation. In the coming years, CERT-EE will need to invest even more in strengthening international cooperation and partnerships, as cybersecurity is a collective task on a global scale," Kupper says, adding that the team is ready to confront new and evolving threats.

'In other words, when most of us are with our families, cyber guards are at work so the rest of the country can enjoy their festive meals.'

The future also points to a more proactive, data-driven approach. "If today the focus is on blocking cyber incidents and attacks, then going forward, CERT-EE will play an increasingly important role in data-driven analysis and prevention. New technologies, such as machine learning and artificial intelligence, enable faster analysis of system behaviour and the detection of even the most complex and covert attack patterns. One thing is certain: CERT-EE has been, and will continue to be, one of the pillars of Estonia's cybersecurity," Kupper said.

RIA OPERATIONS CENTRE begins work

On 1 June 2025, RIA launched its operations centre, whose task is to observe and manage the operation of RIA services and to monitor developments in Estonia's cyberspace. The centre maintains a real-time overview of the digital infrastructure and responds immediately when disruptions are detected.

Monitoring is the core of the operations centre. The monitoring team detects and records cyber incidents around the clock, conducts an initial impact assessment, and coordinates further action.

In addition to technical surveillance, the team also gathers and consolidates other information. For example, every morning it prepares a briefing that provides stakeholders with a snapshot of developments in Estonia's cyberspace over the past 24 hours, along with key cybersecurity developments from around the world.

The monitoring team also monitors RIA's own services and physical security alerts to ensure all systems continue to operate without interruption.

SERVICE OBSERVABILITY

The operations centre ensures that the status of RIA services is visible in real time. This level of situational awareness results from dedicated tools that aggregate data from multiple sources, combined with the expertise to interpret and use that information effectively. The solutions provided by the operations centre are flexible and scalable. They can be expanded and adapted as needed for both smaller and larger systems. An open and transparent approach also helps keep costs under control by avoiding duplication and the creation of expensive bespoke solutions.

As a result, problems can be identified more quickly, responses can be more targeted, and the impact of disruptions can be reduced for both institutions and end users.

CUSTOMER EXPERIENCE AND CUSTOMER SERVICE

One of the operations centre's roles is to communicate with partners and users. The main function of the customer experience team is to resolve user enquiries, analyse customer needs and expectations, collect feedback, and conduct surveys to support service development or address concerns.

Regardless of the client or partner, anyone who contacts RIA should feel that the organisation speaks with one voice. More importantly, enquiries or problems must be resolved as quickly as possible. The operations centre consolidates all enquiries in one place and keeps communication clear and efficient.

DEVELOPMENT OF MANAGEMENT FRAMEWORKS AND PROCESSES

Alongside operational work, the centre also shapes how service portfolio management functions, how IT management processes are designed and how a unified management model is developed. This helps ensure that all services are clearly defined, responsibilities and roles are in place, and activities support both strategic objectives and day-to-day operations.

WHAT COMES NEXT?

To understand the broader impact of incidents on public services and to build situational awareness, the state needs a comprehensive picture. RIA already has a strong foundation for this, built through years of preparatory work.

In 2026, RIA will develop solutions that allow owners of state digital services to automatically transmit information on service availability and disruptions from their monitoring systems to RIA, where it will be consolidated into a single, comprehensive overview. In developing these solutions, RIA places particular importance on making onboarding as simple as possible for institutions.

A SINGLE POINT OF SITUATIONAL AWARENESS

In this role, RIA may be described as a cyber operations centre or a GovSOC (Government Security Operations Centre), but the substance matters more than the name. The resulting situational awareness allows the public sector to better manage and coordinate responses to high-impact cyber incidents. Service owners can also be confident that their critical services are being monitored 24 hours a day.

THE FOUR PILLARS OF THE OPERATIONS CENTRE

- **Monitoring**. We detect and log cyber incidents around the clock.
- **Observability**. We ensure that the status of RIA services is visible in real time.
- **Customer experience**. We resolve user enquiries and analyse customer needs.
- **Development of management frameworks.** We define how services reach users and how they are maintained and developed.

At the same time, it is important to remember that RIA does not replace monitoring by other institutions; it brings the overall picture together in one place. Each institution remains responsible for the availability, integrity and confidentiality of its own services.

WHY IS THIS NEEDED?

RIA's operations centre was established to ensure Estonia's digital state functions without interruption and is ready to respond to both technical failures and cyber threats. Monitoring, service delivery, customer relations and management processes are brought together in one centre. Together, they form a coherent whole that helps make the digital state stronger, more reliable and more transparent. As a result, Estonia's cyberspace and state digital services are protected, managed and trustworthy. Every day. And every night. ●

What did we do in PREVENTION

In 2025, our most extensive prevention campaign was aimed at businesses, helping them recognise cyber threats and protect themselves. We also continued to run workshops for older adults and distributed cybersecurity workbooks to school students.

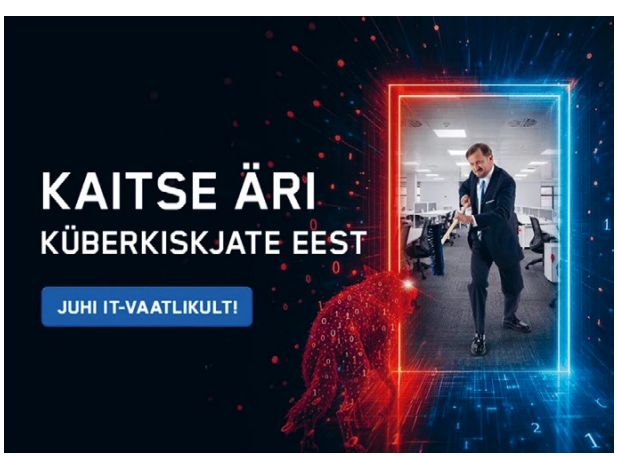
Although cyberattacks targeting individuals are more numerous, the average financial losses tend to be higher when a business falls victim to fraud or cyberattacks.

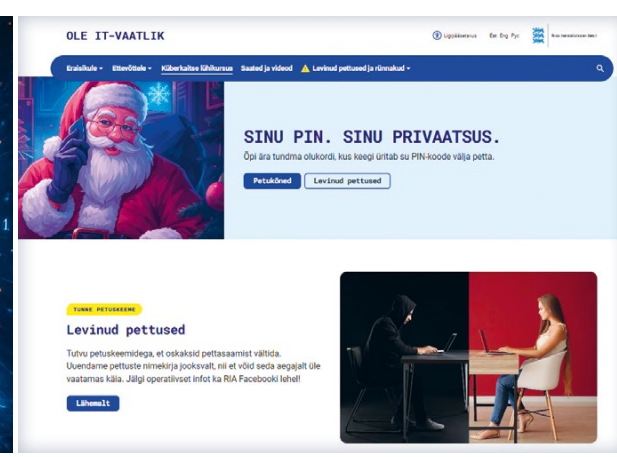
For this reason, our most extensive cybersecurity prevention campaign last year focused on small and medium-sized enterprises. It aimed to raise awareness among business leaders that cybersecurity is a matter of business survival and that responsibility ultimately lies with the chief executive. It is the CEO who decides how company resources are allocated, what kind of organisational culture is fostered and whether employees receive training on cyber risks.

BEC SCHEMES AND RANSOMWARE

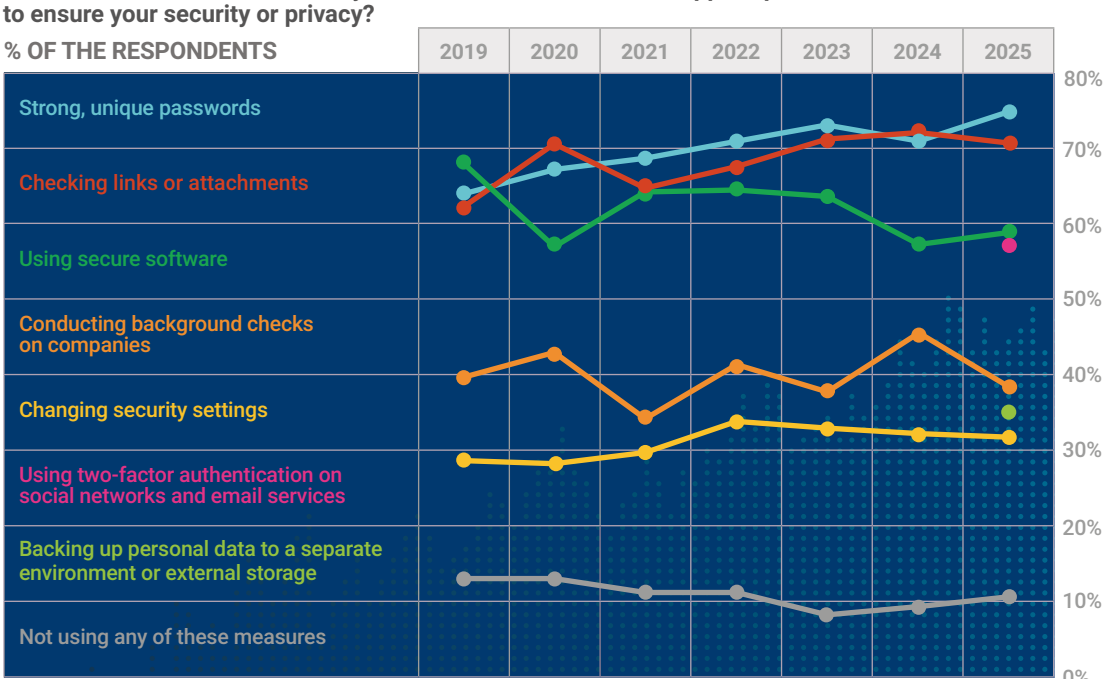
According to our data, Estonian companies suffer the most significant losses from business email compromise (BEC) schemes and ransomware attacks. As part of our prevention campaign, we drew attention to these threats and shared practical guidance on how to avoid becoming a victim. We published articles on the topic, discussed it on the radio and distributed RIA's updated cybersecurity quick guide for businesses.

The campaign proved effective. Follow-up research showed that more than half of those in the target group who noticed the campaign sought additional information or planned to make their companies more cybersecure.





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



Source: Statistics Estonia

The cybersecurity guide for companies, along with information on the scams and attacks that threaten Estonian businesses, is available on RIA's prevention website at itvaatlik.ee.

FOCUS ON SCAMS

The past year saw an increase in scam calls. In response, we ran a campaign at the end of the year to help people recognise attempts to extract their PIN codes. Information on how scam calls are carried out, what warning signs to look for, and when it is essential to end a call is also available on itvaatlik.ee, where we regularly update content on the most common scam schemes.

WORKSHOPS FOR OLDER PEOPLE AND A NEW CYBER TEST

Consistency plays a key role in prevention, and in 2025 we continued several long-standing activities. Cybersecurity workshops for older people remained a core part of our work. Fifteen workshops were held in central and city libraries across Estonia, with nearly 200 participants. The workshops were free, and participants could take home a brochure outlining the fundamentals of cyber hygiene.

In April, a new version of the already well-known RIA's cyber test became available. It was adopted 426 institutions and companies, including state authorities, local governments, schools, hospitals, family medical centres and private companies. By the end of the year, almost 32,000 people had used the test to improve and assess their knowledge.

We also continued distributing cybersecurity workbooks for younger pupils. This autumn, more than 12,000 copies were distributed to schools, teaching children how to navigate the internet safely.

THE YEAR IN NUMBERS

For the seventh consecutive year, we have worked with Statistics Estonia to monitor cyber awareness levels among Estonia's population. The results of the 2025 survey show that people in Estonia continue to prioritise cybersecurity, but practices vary across different areas. The strongest engagement is seen in strengthening passwords and checking the content of unexpected messages, suggesting that people have a good understanding of the most common risks. At the same time, lower scores for adjusting security settings, conducting background checks, and performing regular backups indicate that more technical or time-consuming measures are often neglected and still require greater awareness and habit formation.

How to make PUBLIC SERVICES more resilient

Estonian society relies on convenient public services, but behind them lies a web of dependencies. RIA identifies and strengthens the system's weakest links to ensure services continue to function even when a critical communications cable or power connection fails.

A police officer maintaining public order, a doctor accessing a patient's health data to make treatment decisions, a patient checking issued prescriptions in a national mobile app or a citizen digitally signing a document – all of these are public services. Society expects and needs the most critical services to operate around the clock, seven days a week, 365 days a year – even if cables are cut or whatever the threat may be.

THE MOST CRITICAL SERVICES

The most critical services are those that underpin life and health, public order, the state's situational awareness and, by extension, national security. Equally important are services that keep the lifeblood of the economy flowing.

The functioning of public services is part of everyday life. Digitalisation of Estonia's public services is now near-universal, and interacting online has become the norm. Anything less feels inconvenient and sometimes even impossible. Behind this largely invisible convenience lies a web of dependencies on which Estonian society as a whole relies. These dependencies span both public- and private-sector digital infrastructure.

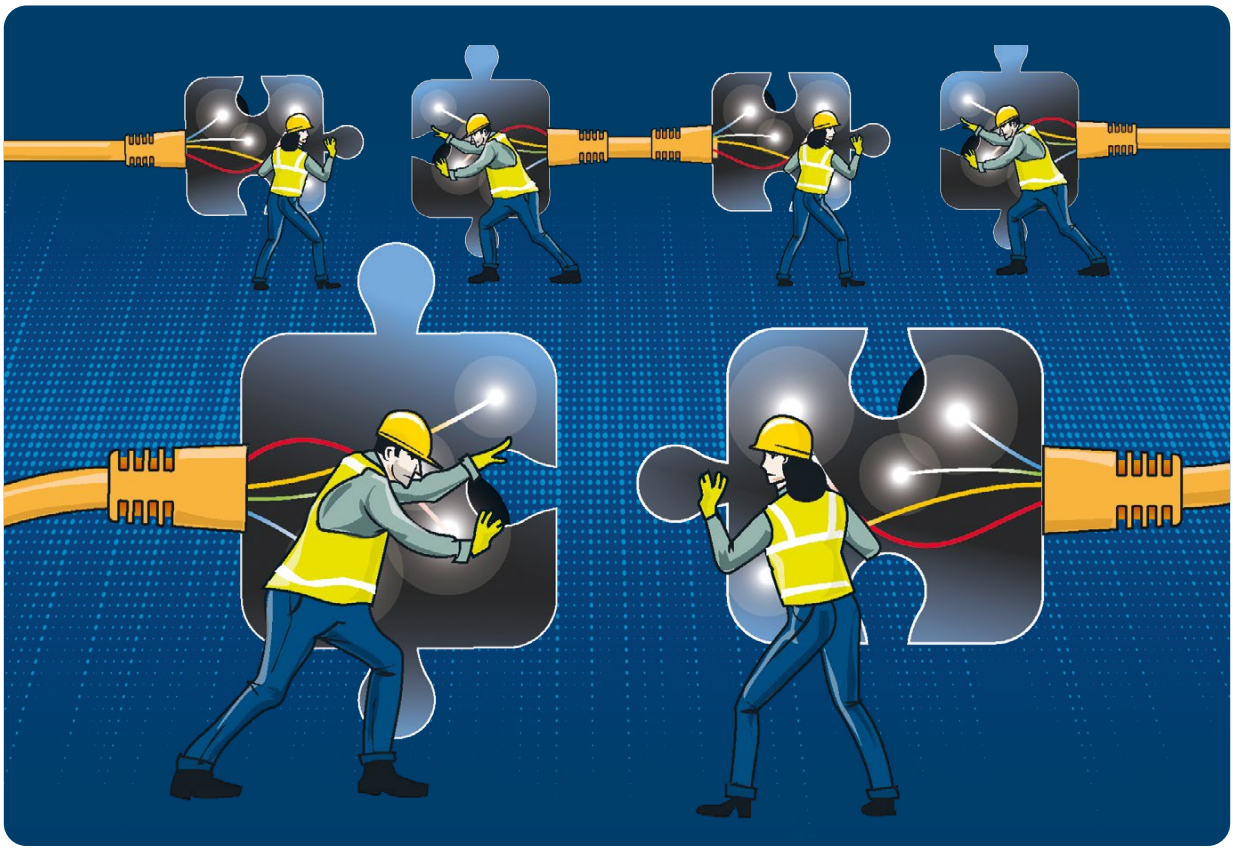
Breaks in subsea cables are a relevant example of incidents that prompt us to act so that society can continue to function as expected under challenging circumstances.

ONE CHAIN, MANY LINKS

To illustrate the situation, it helps to think in terms of a single chain that shows the essential steps required for a service to become usable online. A developer writes the code required to provide the service and then uses an internet connection to install and run it on a remote server. The data centre where the server is located must ensure power supply, data connectivity, cooling and physical security. The end user needs an internet connection at home or on a smartphone.

For all of this to work, numerous technical components must function flawlessly. The closer one looks, the more of these components come into view.

Service resilience improves when each component in the delivery chain has a backup solution. If the power supply fails, a data centre switches to generators; if a communications cable is cut, critical locations rely on redundant connections; to prevent failures in servers and the software running on



them, services are delivered simultaneously from multiple data centres.

RIA PROVIDES THE BACKBONE OF PUBLIC SERVICES

Many public services depend on the central services provided by RIA. In recognition of this responsibility, we invested significantly in improving the resilience of our services in 2025 and will continue this work in the coming years.

This involves creating backup solutions for internal and external dependencies or eliminating dependencies altogether. In physical infrastructure, duplication is key, sometimes in multiple layers. When improving the resilience of software-based services, we reduce dependence on physical infrastructure and its providers. At the same time, we must not compromise on cybersecurity.

Rome was not built in a day, and resilience cannot be improved through a single burst of effort. Choices must be made and priorities set. This process allows us to assess what we, as a state authority, must build and operate ourselves and what makes sense to procure as a fully managed service from other providers, whether in the public or private sector.

Improving the resilience of public services is not the task of RIA alone but of the entire public sector. How successful we are as a country depends on cooperation and on the willingness to revise technological choices and solutions.

Improving the resilience of public services is not the task of RIA alone but of the entire public sector.

PREPARING FOR UNPLEASANT SURPRISES

Good surprises do not require special preparation to respond, but bad ones are easier to manage when preparation is deliberate and systematic. Efforts to strengthen service resilience do not imply that disruptions to the services we take for granted will necessarily become more frequent. We do, however, need to be prepared to address them when they occur.

‘In the worst case, we could be without ELECTRICITY FOR DAYS’

These ominous words were heard during the Cyber Reserve 2025 exercise, where participants, working with Elering, practised responding to a cyberattack that threatened Estonia’s entire electricity supply.

The national power system ensures that our homes are warm and lit, that water flows from the tap, that the internet works from the router, and that food and fuel are available in shops and petrol stations.

Digital control, remote monitoring and automation have made the energy system more efficient, but they also introduce new cyber vulnerabilities that energy security must address.

THE YEAR’S LARGEST CYBER EXERCISE

In 2025, RIA organised a large-scale Cyber Reserve exercise in partnership with system operator Elering, focusing on how to ensure the functioning of

Estonia's energy system during a major cyber incident.

Under the exercise scenario, a real but not yet fully realised threat emerged to the operational continuity of Estonia's electricity transmission network control centres. In the worst-case scenario, such a situation could escalate into a widespread power outage.

The exercise focused on identifying and mitigating risks where an attacker is suspected of having penetrated an organisation's IT systems and may be able to remotely influence transmission network control systems, and on ensuring power system management under extreme conditions.

Nearly 200 experts from close to ten organisations took part in the exercise, which brought together cybersecurity, electricity supply security and crisis management into a single, integrated whole. Participants were given a realistic picture of how a cyber incident could disrupt the power system and what options the state and providers of vital services have to resolve such a situation.

Cyber incidents in the energy sector require rapid and well-considered decisions under conditions of limited information, often with far-reaching consequences.

LEADERSHIP AND DECISION-MAKING IN A CRISIS

A key element of the exercise was practising leadership and decision-making. Cyber incidents in the energy sector require rapid and well-considered decisions under conditions of limited information, often with far-reaching consequences.

Participants were confronted with dilemmas that required balancing system security against the risk of power outages. Responses unfolded in real time and depended on close cooperation between Elering, RIA, other state authorities (including ministries and the Government Office) and Cyber Reserve experts.

SUPPLY SECURITY ALSO DEPENDS ON CYBER RESILIENCE

The exercise confirmed that supply security is not only a matter of physical failures or generation capacity. Cyber threats can affect system control even when physical infrastructure is intact and production matches demand. It is therefore essential that the planning and development of the energy system systematically take cyber risks into account, including their potential impact on frequency control, reserve use and recovery processes.

The exercise underlined the need to maintain and develop the capability to restore the power system even when digital control systems are temporarily disrupted. This requires both technical solutions and people with the necessary know-how, as well as clearly defined roles and responsibilities.

The Cyber Reserve exercise demonstrated how closely intertwined cybersecurity and energy security are. Resolving a high-impact cyber incident demands readiness to act in uncertain and rapidly changing conditions, to make decisions with incomplete information, and to sustain effective cooperation across different organisations. Cooperation builds resilience.

WHAT IS THE ESTONIAN CYBER RESERVE?

The Cyber Reserve is a nationwide network of experts managed and developed by RIA. Its purpose is to support the state and providers of vital services during high-impact cyber incidents. The Cyber Reserve includes more than one hundred experts from across Estonia, drawn from both the public and private sectors, whose knowledge and skills can be deployed when normal resources are no longer sufficient.

Activating the Cyber Reserve requires strong coordination, clear command structures and shared situational awareness. To practise these aspects, RIA organises complex exercises every year that simulate emergencies or imminent threats arising from cyber incidents and test cooperation at both technical and strategic levels.

CYBER-SECURITY reflects organisational maturity

Cybersecurity is often framed as a technical issue – whether a firewall is in place, logs are collected or a risk analysis has been completed. These elements matter, but from a supervisory perspective, they scratch only the surface. In practice, cybersecurity is closely tied to an organisation's overall level of maturity.

Cybersecurity is not merely a technical issue but a matter of management. Where leadership understands information security as a natural part of how the organisation functions, cybersecurity standards are also higher. Where information security is seen as a pointless obligation, an unavoidable nuisance or an external imposition, there is little reason to expect meaningful improvement.

If leadership does not take responsibility, make decisions, allocate resources or explain underlying principles, results will not follow. This applies equally in the public and private sectors, and in both large and small organisations. Documentation may be flawless, policies neatly drafted and audit folders carefully assembled, yet this amounts to only a semblance of information security that provides a false sense of security. In the worst case, this false sense of security quickly leads to an incident.

CYBERSECURITY IS NOT AN EXPENSIVE BOX YOU BUY AND FORGET

We often hear that there is "no money" for cybersecurity. The assumption is that cybersecurity means costly hardware with flashing lights in a server room or cloud services with impressive names. In reality, the issue is not funding but the willingness and ability to think through the problems and follow agreed-upon rules. Asset inventories, clearly defined responsibilities, sensible access management, disciplined backups and change management are activities whose financial cost is often modest.

We still encounter the belief that supervision or audits should focus primarily on the existence of documents. In fact, documents are not for supervisors but for the organisation itself, to explain how processes are meant to work.

The focus of supervision is not on paperwork but on whether processes function in practice. Documentation should exist only to the extent that it describes and supports real activities. A mature organisation uses documents as working tools, while an immature one produces them to appease supervisors or auditors.

STANDARDS DO NOT REPLACE UNDERSTANDING

It makes little difference in practice whether an organisation follows E-ITS, ISO 27001 or another framework, because problems rarely arise from an inability to implement controls. They emerge much

earlier. Organisations often stumble at the asset-identification stage: they do not know what assets they have or how critical those assets are. From there, follow unanswered questions about why and how rigorously they should be protected, and who should make those decisions.

Checks frequently reveal that systems are treated as equal, that all risks are rated medium, and that controls are applied on the basis of a generic checklist rather than informed choice. Only after a serious incident do organisations realise that a system previously regarded as marginal is in fact business-critical.

Risk management is a useful litmus test here. When no distinction is made between risk and threat, when risks are treated as a formal table rather than a decision-making tool, security measures become arbitrary and either under- or over-engineered. In an immature organisation, risk analysis is a dirty word.

RESPONSIBILITY CANNOT BE OUTSOURCED

For smaller organisations, cooperation, joint procurement, and the use of shared or centralised services are often sensible and unavoidable. They make it possible to achieve more, more efficiently.

In supervision, however, we sometimes encounter the mistaken assumption that using a cloud or security service shifts substantive responsibility for information security to the provider. When asked about risk assessment or oversight of the service provider, organisations point to the contract or the provider's reputation. In reality, the provider fulfils the contract but does not make strategic decisions on the organisation's behalf. A mature organisation understands that responsibility remains with it even when services are outsourced.

START WITH YOURSELF

The level of cybersecurity is a direct reflection of organisational maturity: leadership culture, capacity for responsibility, clarity of processes and willingness to make decisions.

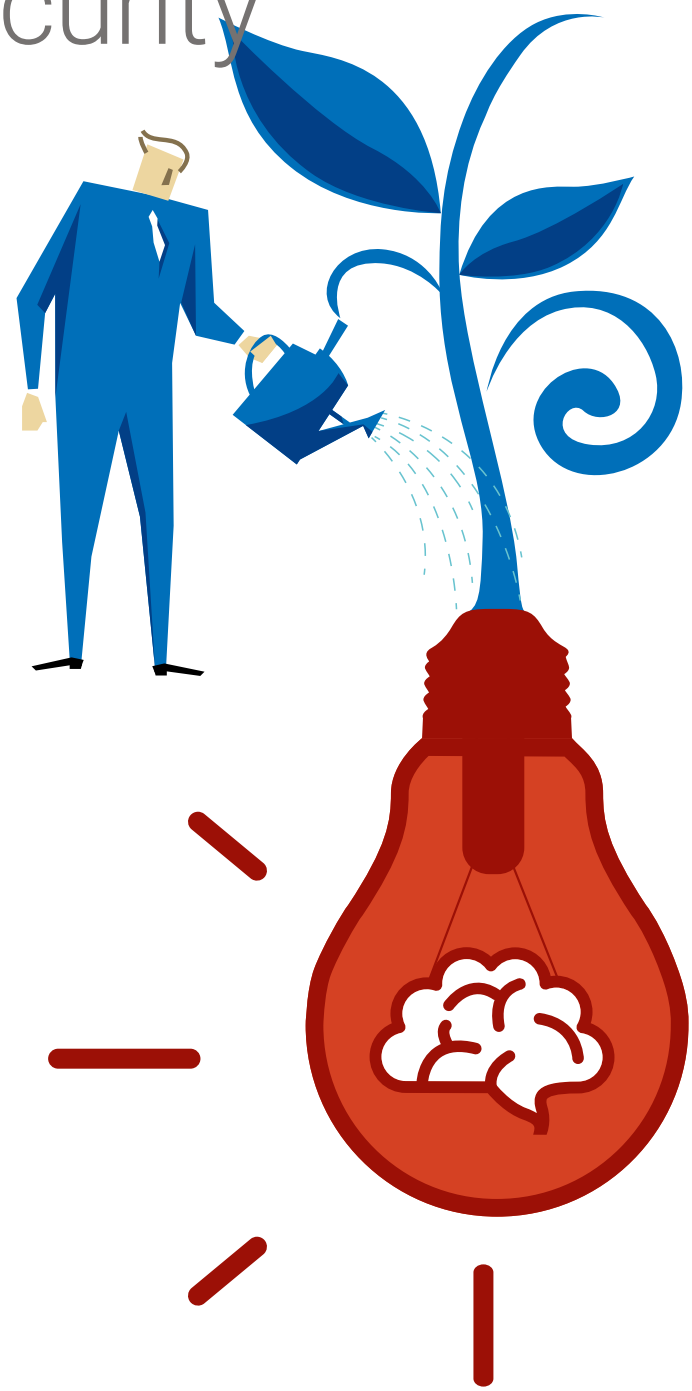
A mature organisation understands what it does, why it does it and who is responsible.

If an organisation wants to improve its cybersecurity posture, it should not start by searching for a new standard or the next technical solution. It should start with itself. A mature organisation understands what it does, why it does it and who is responsible. An immature one deals with symptoms rather than causes. In cybersecurity, this distinction becomes brutally clear.

Responsibility always rests with the organisation itself. When this principle is not understood, problems quickly begin to accumulate. ●

A NEW GRANT for cybersecurity companies

RIA and the Estonian Business and Innovation Agency (EIS) have created a new innovation grant for cybersecurity companies to support product and service development in the sector. Who is it for and how can it be accessed?



The aim of the cyber innovation grant is to help companies take their first step towards working with research and innovation institutions. To receive funding, companies developing cybersecurity services or products must prepare a project proposal in partnership with a research and development institution. This may be a university or a research-intensive company that has participated in a Horizon Europe project. The grant is co-funded by the European Cybersecurity Competence Centre (ECCC) and its members.

UP TO 100,000 EUROS

As the grant ranges from 60,000 to 100,000 euros and the required co-financing rate is 30–50%, depending on company size, the total project budget should be at least 90,000 euros.

A project may include activities such as a proof of concept, the creation or testing of a prototype, the development, testing or demonstration of components, product trials, and an industrial experiment or feasibility study. A single project may also combine several of these activities.

The broader aim is to support product and service development in the field of cybersecurity, while the more specific focus may include automation in cybersecurity, the use of artificial intelligence to enhance cybersecurity, tools that support the transition to quantum-resistant cryptographic algorithms, or technologies linked to the space sector.

As one of the main goals of the cyber innovation grant is to strengthen cooperation between researchers and the business sector, this is reflected in the funding conditions.

FOCUS ON CORE BUSINESS

When drafting the project, it is important to focus on developing the company's core business and consider how collaboration with a researcher could support this through an innovative approach.

The size of the grant indicates that these are only first steps. If the collaboration proves successful, companies can apply for support for larger research, development and innovation projects through EIS applied research programmes or Horizon Europe calls.

As one of the main goals of the cyber innovation grant is to strengthen cooperation between researchers and the business sector, this is reflected in the funding conditions. At least 40% of the total project budget must go to the research and development institution. The company can use the remaining 60% for salaries for its project team, including the recruitment of a doctoral student or a person with a PhD, advisory services such as intellectual property support, metrology, accreditation, certification, or labour and operating costs.

GETTING STARTED

The EIS website provides further information and links to the application process. Before applying, companies are encouraged to identify potential partners to discuss their innovation challenge. Some universities specialise in cryptography, others in artificial intelligence, and some research-intensive companies work in the space sector.

If ideas are plentiful but partners are scarce, companies can contact the research and development coordination unit at RIA's Cybersecurity Centre, which can help identify a suitable partner.

CYBER ACCELERATOR SEEKS NEW START-UPS

Since 2023, RIA's research and development coordination unit and the Tehnopol Startup Incubator have run an acceleration programme for cybersecurity start-ups called the Cyber Accelerator.

As the programme has been extended until 2028, applications will be open in the early summer of both 2026 and 2027 for the next cohort. Each intake welcomes six or seven cybersecurity start-ups. Over seven months, participating companies will receive top-level support from experts and 60,000 euros to develop their idea.

To be eligible, a company must offer cybersecurity products or services. In 2025, the programme focus aligned closely with the themes of the innovation grant: automation in cybersecurity, the use of artificial intelligence to enhance cybersecurity, the transition to quantum-resistant solutions, space technologies and the prevention of manipulation attacks.

The focus areas for 2026 will be announced when applications open. Still, the core aim remains the same: to use new, research-driven solutions to make cybersecurity faster, better and more accessible.

EU CYBERNET moves east

The European Commission has extended EU CyberNet, the EU-funded cybersecurity capacity building project led by RIA, for a further three years. This brings new partners and opens up opportunities to deliver EU assistance in Indo-Pacific region.

EU CyberNet is well known within the Estonian and European cybersecurity communities. Over six years, the project has strengthened global resilience to cyber threats, shared Estonia's experience in building secure digital government services and helped Estonian technology companies open new doors in distant markets. Fewer people are aware that, from spring 2025, the project team worked closely with RIA's management to secure the continuation of the initiative.

In August, those efforts paid off. The European Commission selected the joint bid submitted by RIA and the German Development Cooperation Agency GIZ as the winner for the second phase of EU CyberNet.

SECOND PHASE: NEW PARTNERSHIPS AND BROADER REACH

The second phase of EU CyberNet began in September 2025. RIA contributes technical capacity and cybersecurity expertise, while GIZ brings extensive experience in long-term development cooperation. The addition of a new strategic partner increases EU CyberNet's overall capability but also adds complexity to project management.

During the first phase, EU CyberNet delivered cybersecurity know-how and assistance to Latin America and the Caribbean. Under the new mandate, this support has expanded to the Indian Ocean and Pacific regions, including the Philippines, Indonesia, Thailand, Vietnam, Malaysia, Fiji and others. The challenge is significant, but we believe that prior experience combined with calm and straightforward Nordic approach will help us meet our objectives.

TRAINING AND ADVISORY SUPPORT

EU CyberNet's core activities cover a wide range of training and advisory services. The project has supported newly established computer security incident response teams (CSIRTs), provided advanced technical training for experienced teams, advised governments on cybersecurity strategies and legislation, conducted crisis management exercises and helped partners prepare for international cyber diplomacy forums at the United Nations. Among particular priorities has been investing in the next generation of talent, engaging young people, and promoting gender diversity in cybersecurity career choices.

A significant success story has been the EU CyberNet expert network, which now includes nearly 600 specialists from government, academia and the private sector. Through this network, EU CyberNet has significantly expanded the scope and quality of its technical assistance and is ready to support all cyber capacity building initiatives funded by the EU or its member states worldwide.

LAC4

As part of EU CyberNet, RIA established a regional cybersecurity competence centre for Latin America and the Caribbean, known as LAC4. Based in the Dominican Republic, this training institution now has 16 member states and has become one of the EU's most recognisable brands in the region. It continues its work as a standalone RIA project.

To date, EU CyberNet has delivered more than 250 activities worldwide. Training courses and exercises have involved more than 13,000 participants from more than one hundred countries. In this way, EU CyberNet has operated as an ambassador-like platform for RIA, ensuring sustained international exposure to Estonia's institutional cyber expertise and operational practices.

To date, EU CyberNet has delivered more than 250 activities worldwide.

BUILDING AND SUSTAINING COMMUNITIES

Alongside direct assistance to partner countries, the project portfolio has expanded to include a wide range of activities for the European Commission and EU institutions. These include community meetings for EU-funded cyber projects, monthly EU CyberNet Club events, expert short courses and summer schools. Such initiatives foster the exchange of knowledge and good practice and contribute to the development of EU cyber capabilities.

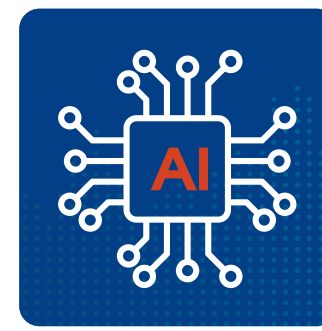
The project's website hosts a mapping tool developed primarily for the European Commission, which provides an up-to-date overview of all EU-funded cyber-capacity building initiatives worldwide. This consolidated view enables better coordination and strategic planning at the EU level and reduces the risk of funding overlapping activities.

Cyberspace IN 2026

AI IS ACCELERATING ON ALL FRONTS

The development of artificial intelligence (AI) and large language models (LLMs) continues at a breakneck pace. These technologies certainly make everyday life easier by allowing increasingly complex questions to be asked and more informed answers to be obtained. At the same time, they also benefit criminals and aggressive regimes, who can use AI to target their objectives more effectively.

In 2025, our Ukrainian partners observed Russia deploying malware that uses internal AI algorithms. Russian state-backed threat actors also began using malware capable of generating malicious commands autonomously in attacks against foreign governments and armed forces. Last year also saw the market entry of a cost-effective and technically capable Chinese language model, known as DeepSeek. For now, the primary concern is not its use in attacks against neighbours or other states but the sharing of data entered into DeepSeek with various Chinese



government and security authorities. We highlighted the risks arising from this repeatedly in 2025 and will continue to do so this year.

EVOLVING LEGISLATION BRINGS CYBERSECURITY INTO FOCUS

Amendments to Estonia's Cybersecurity Act entered into force on 1 January 2026, incorporating the European Union's second Directive on the Security of Network and Information Systems (NIS2) into Estonian law. As a result, the number of Estonian companies and institutions required to comply with the new requirements rose from around 3,500 to nearly 6,500. The directive aims to raise cybersecurity standards across the entire European Union.

The new legal framework introduces personal liability for board members for compliance with cybersecurity requirements and significantly higher potential fines for breaches – up to 10 million euros or two per cent of annual turnover. Cybersecurity is therefore moving much higher on the radar of organisational leadership.

Under the previous version of the Estonian Cybersecurity Act, all entities within its scope were required to comply with the Estonian Information Security Standard (E-ITS), which supports larger and more capable organisations in managing information security in a structured way. With the recent amendments, smaller organisations are now met halfway: they are required to implement only the general requirements, or primary information security measures,

defined by RIA in 2025. These significantly reduce the administrative burden and focus on a limited set of essential, realistic measures that reflect the size, resources and risk profile of smaller entities. This should lead to a sharp increase in the number of small organisations that genuinely seek to implement information security in practice.

ANOTHER RECORD YEAR FOR INCIDENTS WITH AN IMPACT

In 2025, yet another all-time high in the number of incidents with an impact was recorded in Estonia's cyberspace. The total reached 10,185, marking the first time the figure has risen to five digits within a single calendar year. In 2024, the number was around a third lower, and the year before that, it was almost three times smaller. Given the pace at which increasingly capable cybercriminals continue to devise new and effective fraud schemes, we must unfortunately expect this upward trend to

continue in 2026. Growth is unlikely to be as steep as last year, but the basics still apply: do not click every link, and never enter PIN codes in response to an unexpected phone call. If you do fall victim to a cyber incident, please report it by email at **cert@cert.ee** or by completing the report form at **raport.cert.ee**.

A NEW LEVEL OF NORDIC–BALTIC REGIONAL CYBER COOPERATION

In December 2025, the Nordic Baltic Cyber Consortium (NBCC), launched under Danish leadership, began substantive work. Seven countries are involved: Estonia, represented by RIA, alongside Latvia, Lithuania, Finland, Denmark, Norway and Iceland. Sweden is expected to join the consortium at a later stage.

The purpose of the NBCC is to strengthen regional cooperation and improve the prevention and detection of cyberattacks. This will involve developing shared tools for information sharing and analysis and enhancing cyber threat awareness by drawing on information sources from both the public and private sectors. The consortium also emphasises innovation and public–private cooperation.

This cross-border effort is supported by the European Union

through the Digital Europe programme, with a total project budget of around 14 million euros over four years. In the context of the EU Cyber Solidarity Act, the NBCC initiative serves as a cross-border cyber hub. The network is expected to actively exchange information with similar hubs across the EU, forming part of a pan-European cybersecurity early warning system.

FURTHER CENTRALISING CYBER DEFENCE

RIA's new operations centre began work on 1 June 2025, taking over responsibility for monitoring Estonia's cyberspace from CERT-EE and for the real-time oversight and management of RIA's own services. The operations centre functions as RIA's central nervous system, acting as an emergency hub when threats arise. It was created to ensure that Estonia's digital state continues to operate without disruption and is ready to respond immediately to both technical failures and cyber threats.

In 2026, this capability will be extended to other state e-services, with the aim of building a more complete view of activity across Estonia's cyberspace. User-friendly solutions will be introduced that allow service owners to automatically share service availability and disruption information from their monitoring systems with RIA.

In this role, RIA will increasingly function as a government security operations centre, or GovSOC. The consolidated situational awareness gathered at RIA will enable more effective management and coordination of responses to high-impact cyber incidents, while ensuring round-the-clock oversight of national critical services.

CYBER SECURITY IN ESTONIA 2026

Publisher: **Information System Authority**
Pärnu mnt 139a, 11317 Tallinn
Design: **Martin Mileiko** (Profimeedia)
Illustrations: **Andres Varustin, Martin Mileiko**
Translation: **Margus Elings** (Refiner)
Editing: **Scott Abel** (Tekstikoda)
Print: **K-Print**
ISSN 3059-877X

Read more: **ria.ee/en** & **itvaatlik.ee/en**