2025 Q4

LATVIAN CYBERSPACE SITUATION

PERIOD: 01.10.2025–31.12.2025

CERT.LV
Cyber Incident Response Institution

Institute of Mathematics and Computer Science University of Latvia

Ministry of Defence Republic of Latvia

Summary

The level of cyber threats in Latvia remains **high, with a steady upward trend**. Since Russia's full-scale invasion of Ukraine, the number of **cyber incidents** in Latvian cyberspace has increased **sixfold**. In Q4 2025, a historically highest number of manually processed cyber incidents by CERT.LV was recorded (923), while **the number of compromised devices increased eightfold**, **reaching a record high** of 731,783 during the reporting period.

Attacks are both financially and politically motivated, and geopolitical factors continue to serve as a significant catalyst for threats. It is not just the intensity and complexity of attacks that are increasing: it is also the ability of attackers to adapt, which in turn encourages the development of appropriate tech security solutions, spurring demand for data-driven services and for better response capability in the public and private sectors.

In Q4 2025, **fraud was the dominant driver** behind the growth of cyber incidents in Latvian cyberspace, creating significant and increasing financial risks for both individuals and organisations. Social engineering activities are intensifying through the effective use of artificial intelligence tools and automation, accelerating identity theft and account compromise.

CERT.LV proactively monitors fraud campaigns, and highly values public involvement in identifying and reporting fraudulent websites. Reports received are aggregated, and malicious domain names are added to **the DNS firewall. During the reporting period, the DNS firewall protected users from visiting malicious websites 1.03 million times**, indicating a **record-high intensity of fraud campaigns**.

At the same time, the increase in fraud-related damage nationwide, particularly outside bank payment channels, highlights a **critical need to strengthen public digital literacy and resilience**, as well as the role of electronic communications operators in preventing telephone fraud.

The exploitation of vulnerabilities and the rapid growth in the number of compromised devices indicate the escalation of botnets, infected end-user devices and weak configurations, increasing the risk of further targeted attacks.

Significant risks are posed by denial-of-service (DDoS) attacks targeting state institutions, information and communication technology (ICT for short) critical infrastructure and service providers. The primary objectives of cyber-threat activities by Russia-aligned hacktivists in Latvia are to reduce Latvia's support for Ukraine. Incidents recorded to date have not caused significant or lasting impacts on essential public functions, indicating the effectiveness of existing protective measures.

Cyber-espionage threats persist and may potentially be linked to Russia. Interest in Latvia's ICT critical infrastructure from Chinese and Belarusian-backed cyber attackers has not diminished. **Indirect risks are increasing, particularly those related to supply chains** and the use of external service providers as the most common **"backdoor" to target infrastructure**.

Although Latvia's cybersecurity regulatory framework is becoming more structured overall, **the automation of cyber threats and the increasing pace of cyber attacks increasingly challenge organisations' ability to identify attacks in a timely manner**. Faster and more effective detection of cyber threats is achieved by combining 24/7 monitoring of the cyberspace situation, oversight provided by the Security Operations Centre (SOC for short), proactive threat hunting, and targeted strengthening of the human factor and supply chain security.

Contents

1. Cybersecurity threats: statistics and trends

Dynamics of cyber incidents and compromised devices

In Q4 2025, Latvia recorded a **historically highest number of manually processed cyber incidents[1] in total – 923** incidents, which represents **a +62%** increase compared to Q4 2024 and **a +38%** increase compared to Q3 2025.

Since the start of the war launched by Russia in Ukraine, the number of cyber incidents in Latvian cyberspace has increased sixfold, with a persistent upward trend. This indicates an increased manual analysis workload both for the CERT.LV cyber incident response and SOC teams, as well as for the incident handling ecosystem as a whole.

At the same time, this correlates with a sharp and **historically unprecedented increase in the number of identified compromised devices** – since 2022, the number of threats has increased eightfold. The year 2025 marks a quantitative tipping point, where the volume of cyber incidents no longer increases linearly, but instead surges sharply, reaching **731,783** in Q4, which represents a **+141%** increase compared to Q4 2024 and a +**17%** increase compared to Q3 2025.

This indicates an increase in automated botnet attacks and automated scanning, exploitation of vulnerabilities and configuration weaknesses, and highlights the need to prioritise a proactive cybersecurity approach – early threat detection and capacity building, in order to reduce the risk of incident escalation and impact.

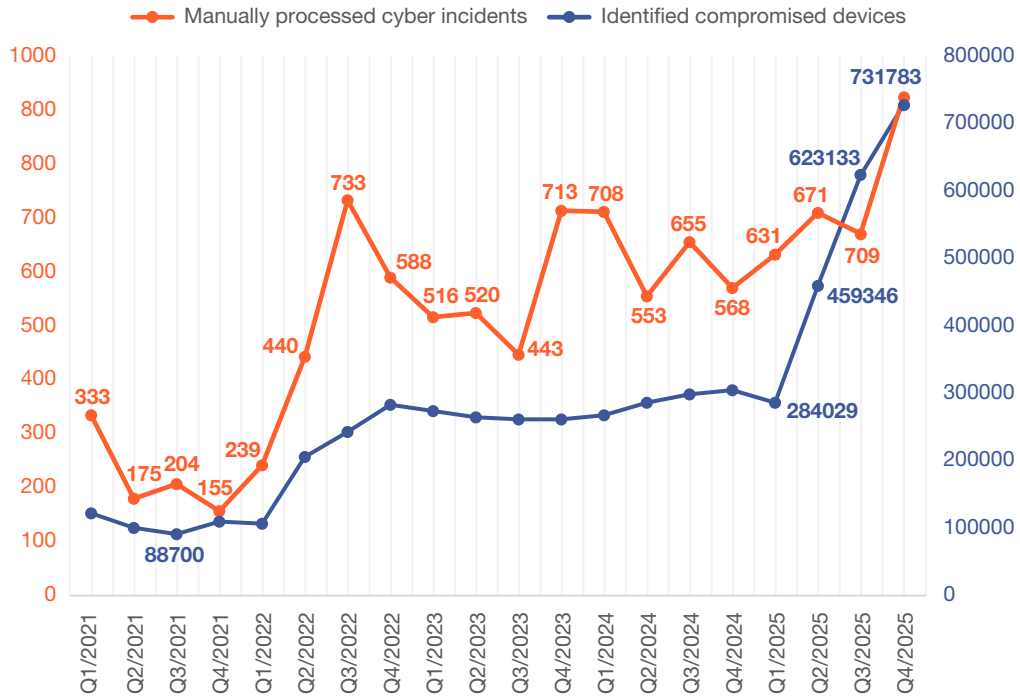


Figure 1. Dynamics of cyber incidents and identified compromised devices (per quarter; 2021-2025)

The range of attacks is broad and includes:

- activities of state-backed groups;
- financially motivated cyber attacks;

There are several positive examples of incidents that could have occurred but did not, because the CERT.LV team detected and mitigated vulnerabilities at an early stage through timely penetration testing, thereby preventing the risk of significant cyber incidents.

1 Events that threatened data processed or the availability, authenticity, integrity, or confidentiality of services offered by or accessible through network and information systems.

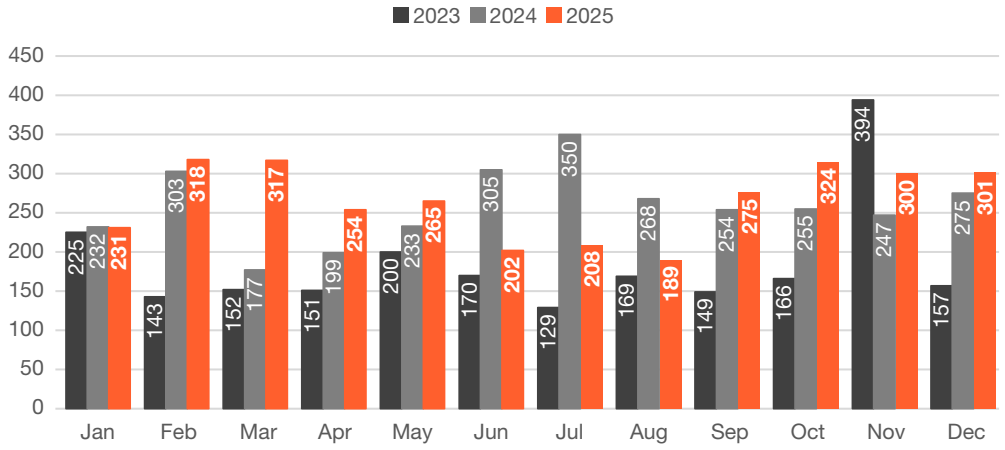


Figure 2. Cyber incident trends (monthly breakdown)

During the reporting period, the number of manually processed cyber incidents by month has overall been relatively stable and high, which is characteristic of the end of the year and the holiday season, when discounts and "special offers" become more frequent, and fraudsters also become more active. This means elevated threats and requires particular vigilance.

CERT.LV cyber incident response and SOC teams demonstrate a high level of readiness and ability to respond to various cybersecurity challenges on a daily basis, providing the necessary support to organisations and private individuals.

Subjects of the National Cybersecurity Law (NCL for short) that use CERT.LV services, including SOC services, are able to detect threats faster and mitigate them more effectively.

Recommendations for organisational ICT security

- **Regularly carry out a comprehensive inventory of devices and systems to obtain a complete overview of the infrastructure, in order to timely detect and mitigate risks caused by outdated or unprotected equipment.**
- **Avoid unnecessary exposure of IT resources to the public internet, providing access only through secure solutions, using multi-factor authentication solutions (MFA / 2FA) or encryption.**
- **Regularly follow software updates, promptly installing the latest available security patches for all systems.**
- **Implement centralised update management, ensuring continuous monitoring across all systems.**
- **Regularly perform vulnerability scanning to identify weaknesses and reduce risks from known vulnerabilities.**

For "cyber weather" observers, CERT.LV offers a monthly report in simple language on the most significant and striking cyber incidents and threats in Latvian cyberspace in the TOP 5 categories. The report is available on the CERT.LV website OCTOBER | NOVEMBER | DECEMBER

2. Top reporting-period cyber threats and key events

Analysis of cyber threat structures by incident type

An increase is observed in most types of cyber incidents compared to 2024, while compared to Q3 2025 the picture is uneven – some risks increase, others decrease.

- **The dominant type of incident is fraud**, which constitutes the absolute majority and determines the overall growth dynamics. Trends indicate mass use of social engineering and artificial intelligence (AI) tools for automation and content creation.
- **Technical attacks** (intrusions, malware) have largely stagnated in absolute numbers, while at the technical level, **new and dangerous social engineering and malware campaigns** have emerged, particularly the evolution of the "ClickFix" method. Incidents were recorded in the Microsoft 365 environment where attackers **were able to bypass multi-factor authentication** (MFA). Financially motivated attackers actively use **"infostealer" type data-stealing malware** to extract user authentication data.
- **Both the number of compromised devices and availability disruptions (hereinafter – DDoS) are rapidly increasing** quarter-on-quarter, indicating a growing automated threat background. In most cases, DDoS attacks occur without affecting service operation and are repelled automatically. The Ministry of Defence funds a centralised DDoS protection service, which is available to state administration institutions free of charge. The provision of the service is delegated to the "Latvia State Radio and Television Centre".
- CERT.LV cybersecurity threat hunting results indicate that **attackers often use outsourcing providers as an initial access point to target infrastructure**, which then becomes a "bridge" for further attacks. **Similar approaches are also used in the software ecosystem** to insert malware or manipulate the software supply chain, using trusted channels and development environments.

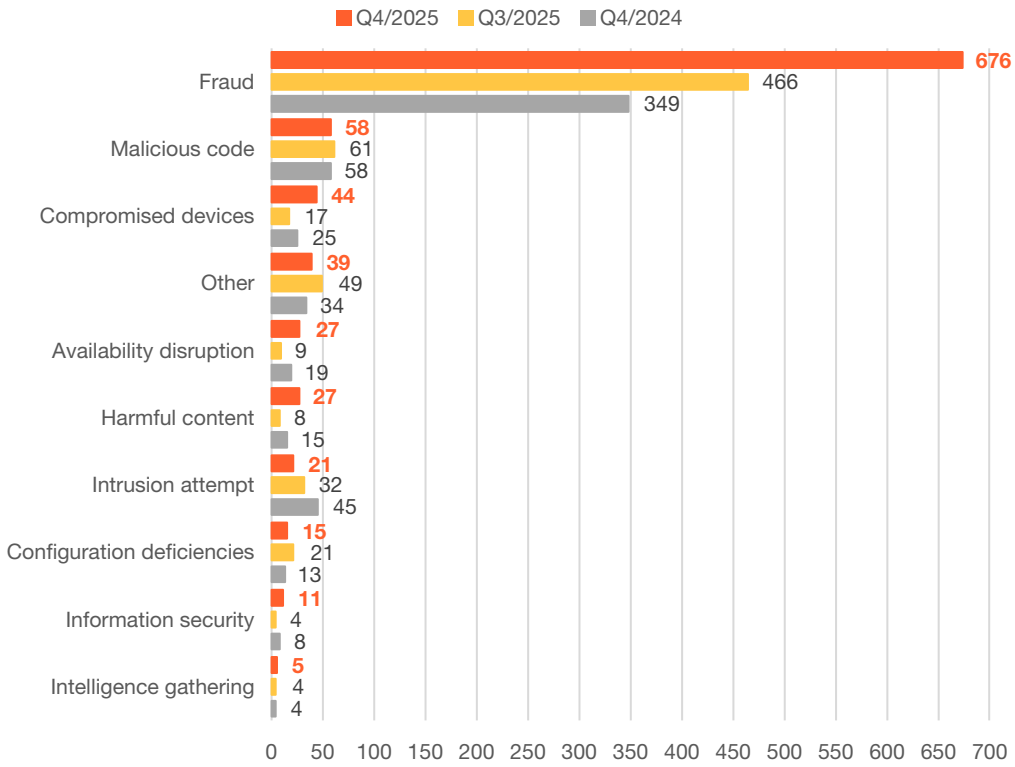


Figure 3. Comparison of cyber incident types and numbers

TOP 6 quantitatively largest types of cyber threats

Threat type: number of manually processed incidents in Q4 2025	Change relative to Q4 2024	Change relative to Q3 2025	Key conclusions
FRAUD: **676**	+94%	+45%	► **Very rapid and persistent growth**, indicating intensive social engineering campaigns. Active phishing, smishing and telephone fraud have been observed. **Investment fraud** dominated, using fake websites with misleading articles about "profitable investment opportunities", where images of publicly recognisable persons (for example, the Prime Minister and others) were maliciously used to create an illusion of credibility.
MALICIOUS CODE: **58**	No change	-5%	► The volume remains large and stable, with persistent malware risks. A **dangerous evolution of social engineering** and **the "ClickFix" method** (where the user is encouraged to "fix" an allegedly occurring problem themselves) was observed. ► **Data-stealing malware** that steals passwords, cookies and other data is one of the **fastest-growing** types of cyber threats. ► Malware statistics clearly reflect issues related to **SOHO** and **Edge network device vulnerabilities** – several of the most common malware families are directly linked to the compromise of small routers and other Edge devices.
COMPROMISED DEVICES: **44**	+76%	+159%	► A very rapid quarter-on-quarter increase has been observed, indicating expansion of **botnets**, **an increase in infected end devices and widespread incorrectly or inadequately configured systems**. Such dynamics may serve as a precondition for further cyber attacks.
AVAILABILITY DISRUPTIONS: **27**	+42%	+200%	► A significant increase is observed, especially compared to Q3 2025, although the absolute number remains moderate. ► Not every service disruption is a DDoS attack – in some cases, it was caused by **configuration errors**, indicating the **need to improve testing procedures**. ► The global Cloudflare service disruption experienced in November caused a cascading effect, affecting the operation of many websites and digital services also in Latvia. This incident clearly demonstrates – **reliance on a single solution increases risk**, as an outage can cause widespread service unavailability and trigger a chain reaction – websites and services become partially or even fully unavailable.
HARMFUL CONTENT: **27**	+80%	+238%	► A sharp increase is observed, although the absolute number remains moderate. The increase is largely linked to fraudulent, malicious web content that overlaps with fraud trends.
CONFIGURATION DEFICIENCIES: **15**	+15%	-29%	► A quarter-on-quarter decrease has been observed, possibly indicating improved cyber hygiene practices, however risks remain. ► **High risk exists both for end users** (7-Zip, Chromium browsers, Redis, etc.) and for **critical infrastructure** (FortiWeb, Ubiquiti UniFi Access, Squid, etc.). ► Critical remote code execution **(RCE) vulnerabilities dominate in widely used technologies**, allowing attackers to gain full control over systems. ► A visible trend has been observed – **multiple vulnerabilities are combined** in attacks to bypass defence mechanisms.

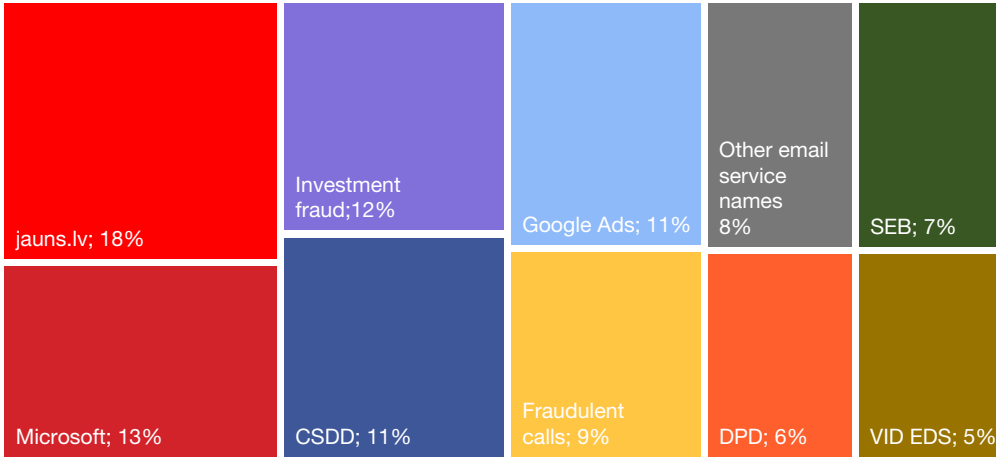


Figure 4. Most common fraud campaigns using organisation names (percentage of total number of phishing messages processed by CERT.LV in Q4 2025)

A trend is being observed – fraud campaigns are becoming increasingly shorter, more precisely targeted and contextually adapted. Names and processes of well-known organisations are used, focusing precisely on what sounds "credible" at a given moment.

During the reporting period, fake websites imitating real sites, such as jauns.lv, were most frequently used, disseminating misleading advertising articles that used images of well-known public figures to create credibility for fraudulent investment offers.

In phishing campaigns, the placement of Google Ads sponsored pages in Google search results was actively used to redirect users to fraudulent pages. For example, when entering the word "ibanka" in Google search, the first (sponsored) search results were fake pages created by fraudsters that visually resembled SEB Bank's internet banking.

Fraudulent campaigns conducted in the name of public authorities (especially CSDD) were recorded; fraudulent calls impersonating representatives of various organisations increased; smishing cases in the name of delivery companies were observed, as well as other types of fraud.

Impact assessment

- During holiday and sales periods, the risks of financial losses are significantly increased by fraudulent campaigns, fake websites, account compromise and user inattention under conditions of heightened activity and urgency.
- Personal data and identity theft, as well as user account compromise, are widespread.
- Deficiencies in public awareness and digital literacy remain significant.

According to information from the State Police, in the first 10 months of 2025, residents' losses due to fraud reached EUR 17.99 million.

Data from the Finance Latvia Association shows that in the first 11 months of 2025, financial fraudsters managed to swindle EUR 10.954 million from Latvian residents, which is 26% less than in the corresponding period last year. At the same time, banks managed to protect residents from losses amounting to EUR 12.749 million.

This indicates an increase in the effectiveness of banks' preventive measures, but at the same time points to an overall increase in damage caused by fraud in the country, especially outside bank payment channels. Moreover, in cases of telephone fraud, the amount of funds defrauded reached almost EUR 5.91 million, indicating a critical need to strengthen the role of electronic communications operators in preventing telephone fraud.

The statistics provided by the State Police and the Finance Latvia Association differ, as the Finance Latvia Association's data only covers participants in the Latvian financial market, whereas the State Police statistics also include activity outside Latvian financial institutions.

5 simple steps for user security in the digital environment

- **Use strong, unique passwords and enable multi-factor authentication (MFA / 2FA) wherever possible.**
- **Update operating systems, applications and browsers in a timely manner.**
- **Do not open suspicious links and attachments (especially if they create a sense of urgency).**
- **Limit the use of public Wi-Fi or use a VPN when accessing sensitive accounts.**
- **Use the DNS firewall mobile application.**

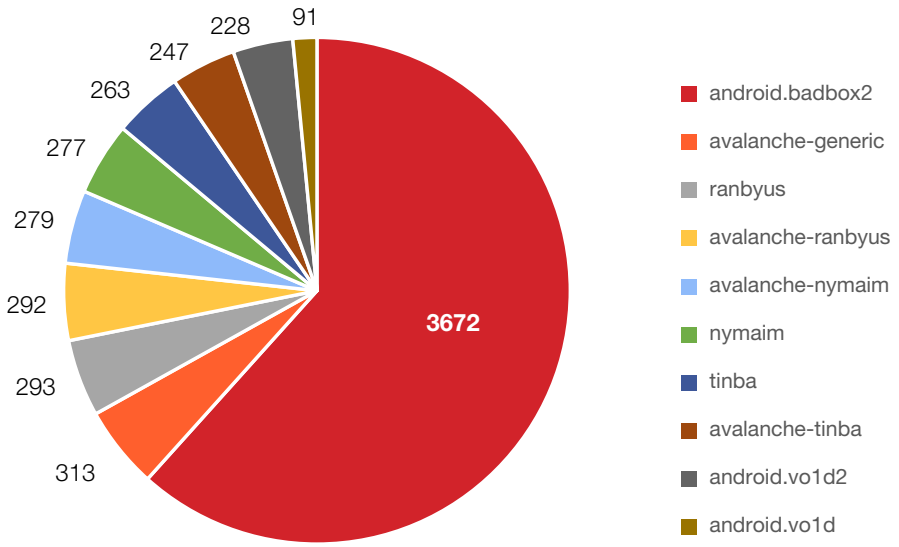


Figure 5. Top 10 malware in Q4 2025, by number

TOP 10 malware

The most widespread malware types in Q4 2025 indicate large-scale, automated and persistent threats.

- At the top of the malware TOP 10, the “Android.badbox2” malware clearly dominates; it is a mobile botnet variant capable of infecting devices by, for example, stealing access credentials and enabling remote control of the device. Its spread indicates significant and targeted activity on Android devices and points to mass infection campaigns using unofficial app installations or fake updates.
- The main risks are interception of access credentials, compromise of infected end devices and their use in subsequent cyber attacks. Organisations and individual users may not even be aware that their IP address is “participating” in botnet attacks.
- The remaining top malware together account for a quantitatively smaller share; however, they demonstrate a diverse combination of attack vectors and increase compromise risks.

The most common types of malware

- **User data-stealing malware**
- **Botnets**
- **Remote control trojans for data extraction and infrastructure compromise**

“Infostealer” type data-stealing malware is used to extract access credentials from web browsers or unencrypted files. This type of malware is distributed as a malicious web browser plugin or as an executable file attached to a phishing e-mail.

State-backed cyber attackers

Russia	► Russian-backed attackers (APT – Advanced Persistent Threat) are expanding their activities and conducting cyber operations more broadly than before; however, the overall quality of attacks has declined, indicating a decrease in attacker professionalism, while at the same time pointing to an increasing scale and volume of attempts to influence cyberspace. ► Russia remains the main source of threats in the region, combining technical attacks with information influence; moreover, any means capable of causing harm is considered acceptable and usable.
Belarus	► A less significant player, mainly involved in episodic campaigns, most likely orchestrated by Russia. ► Activities are more related to influencing the information space and less often to technically sophisticated cyber operations.
China (PRC)	► Groups associated with the PRC are increasingly being observed in Latvia. ► Whereas previously they mainly exploited vulnerabilities in Edge network devices (VPN gateways, firewalls, etc.) to gain initial access, now a more targeted and aggressive spread within networks is being observed.

Western countries, including Latvia, are facing sabotage attempts against their critical infrastructure assets. Russia and Belarus **use operational technologies (OT) as weapons against Western countries** – energy, water and heating infrastructure, as well as **drones and other unmanned platforms**, to destabilise the social and economic environment.

Although cybercriminals are most often the perpetrators of cyber attacks, state-backed groups also continue to target strategically important sectors, **primarily for espionage purposes, but often also for financial gain**.

APT attacks are carried out according to defined patterns, and increasingly they can be anticipated and **responded to appropriately by developing deterrence capabilities**, **making Latvia a less convenient target for attackers**.

Main conclusions

Geopolitical and ideological conflicts remain a strong catalyst for cyber attacks. The increasing activity of cybercrime and an ever broader range of cyber threats, intensified by the use of AI tools and automation, have contributed to an increase in the number of cyber incidents also in Latvia, particularly in the categories of fraud, compromised devices and automated attacks.

Incidents recorded to date have not caused significant or lasting impacts on essential public functions, indicating the effectiveness of existing protective measures. At the same time, the increase in damage caused by fraud in the country, especially outside bank payment channels, points to a critical need to strengthen public digital literacy and resilience. It is also essential to strengthen the role of electronic communications operators in preventing telephone call fraud.

Despite relatively strong regulatory frameworks, available technologies and state support for strengthening defence capabilities, the risk of threats remains high.

At the individual level, the use of multi-factor authentication (MFA / 2FA) and understanding of the importance of cyber hygiene should be promoted, which can significantly reduce the risks of fraud, personal data leakage and account compromise.

Sustainable organisational resilience can only be ensured through a multi-layered approach in which cybersecurity is integrated into organisations' strategic management decisions, daily operational activities and user behaviour, combining technological solutions, SOC 24/7 monitoring, regular testing and targeted employee training. This helps to significantly reduce both the likelihood of cyber incidents and their impact on business continuity, sensitive data, reputation and financial stability.

3. CERT.LV services: monitoring, protection and testing

CERT.LV services, including the DNS firewall, incident response support, SOC 24/7 monitoring, cybersecurity threat hunting, security testing, public education and training, etc., provide essential support for risk mitigation and strengthening resilience against growing cyber threats. Meanwhile, the cybersecurity regulatory framework developed by the Ministry of Defence provides a cooperation framework that defines responsibilities, obligations and minimum requirements for NCL subjects.

DNS firewall

In Q4 2025 blocks by all lists maintained by the CERT.LV DNS firewall **protected users from visiting malicious websites 1,028,577 times**, which is a significant increase – by **158%** more than in Q3 2025 and by **124%** more than in Q4 last year (the reporting period statistics do not include data from lists of other competent state authorities restricting illegal online content).

Possible reasons for the increase include seasonal and contextual factors, and the number of blocks is directly influenced by the number of active fraud campaigns.

CERT.LV proactively monitors and promptly stops fraudulent campaigns, and at the same time positively assesses the involvement of residents who identify and forward fraudulent e-mails and websites to cert@cert.lv. The received reports are compiled, and malicious domain names are added to the DNS firewall in order to restrict access by Latvian internet users and reduce potential damage.

Sensor Network

The Cybersecurity Early Warning System (EWS) is a service provided by CERT.LV that analyses traffic anomalies and identifies signs of cyber-attacks in the service recipient's infrastructure. CERT.LV continues to maintain and expand the EWS system.

In Q4 2025, the number of ABS-generated alerts was approximately 800 million, which is less than in the previous quarter. The decrease in volume is explained by optimisation of the indicator set used.

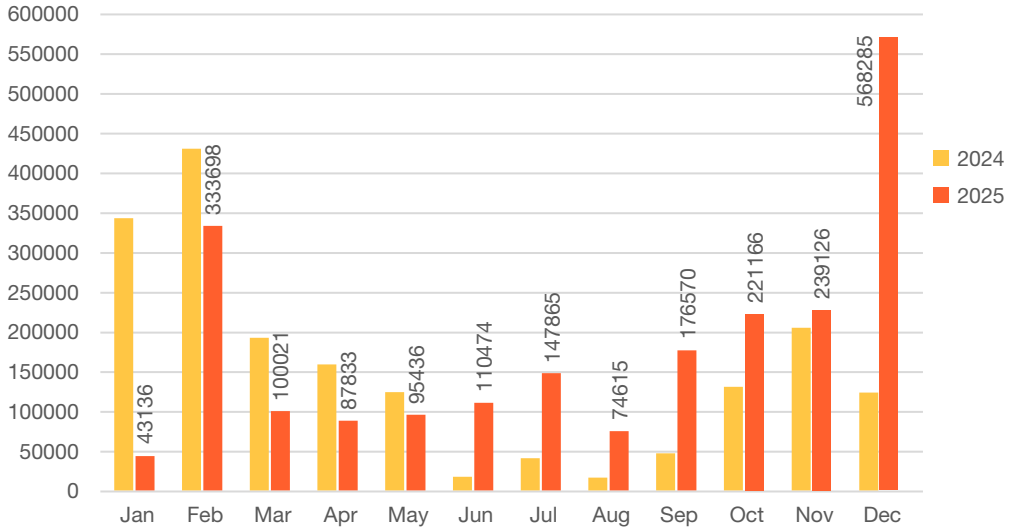


Figure 6. Blocks by all lists maintained by the CERT.LV DNS firewall that protected users from visiting malicious websites

On average, the EWS records **6 000** high-priority cyber threats (incidents with high danger potential) per month in state, local government and ICT critical infrastructure organisations.

> 2.2 million – number of blocks by lists maintained by the CERT.LV DNS firewall in 2025 (an increase of +20% compared to 2024)

~75,000 – total downloads of the DNS firewall mobile application on Android and iOS devices (since 2024, when the application was introduced)

~30 min – average response time until identification and inclusion of the indicator in the blocking list

~13.1 million – total DNS queries for malicious domain names in 2025

Security Operations Centre (SOC)

CERT.LV continues to develop SOC services and attract new clients, expanding the client base in line with the NCL and promoting more effective 24/7 protection and resilience against cyber threats.

As of the end of the reporting period (31.12.2025), 55 NCL subjects use CERT.LV SOC services.

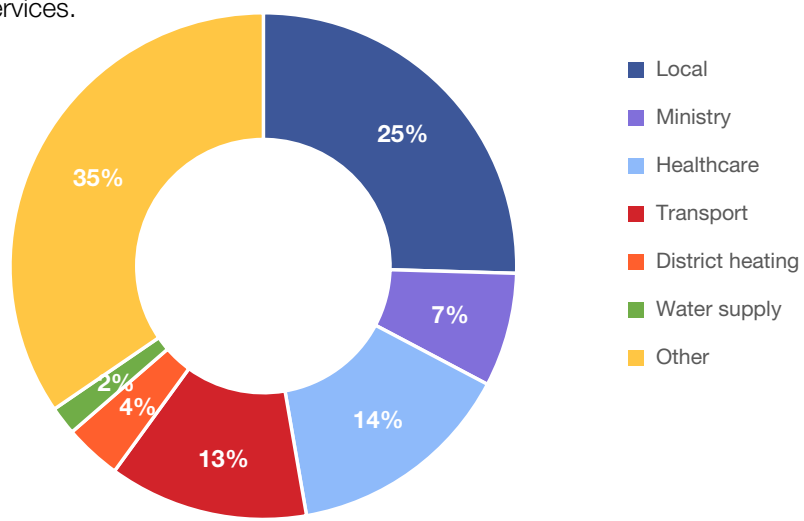


Figure 7. Percentage breakdown by institution sectors using the CERT.LV SOC service

Dynamics of security alert reports in CERT.LV SOC client infrastructure

	Total
Number of alert reports	**23M+**
Manually created cases	**689**
False positive cases	**521**
Number of incidents	**8**
Low level of alert	**6,8M+**
Medium	**16,5M+**
High	**79k+**
Critical	**53k+**

Overview of security alert reports

- **Visibility was obtained over a total of 41,534 end devices**, including servers and workstations. In Q4 2025, visibility was obtained over 814 end devices (an increase of +2% of the total volume), and accordingly the number of security alert reports also increased.
- **More than 23 million security alert reports** – a +57% increase in Q4 2025 compared to Q3 2025. The increase is explained by broader visibility obtained in the infrastructure of new clients and the time required to process alert reports in order to investigate and suppress false positives.
- **689 manually created cases** – a +40% increase in Q4 2025 compared to Q3, when processing security alert reports.
- **681 false positive cases**

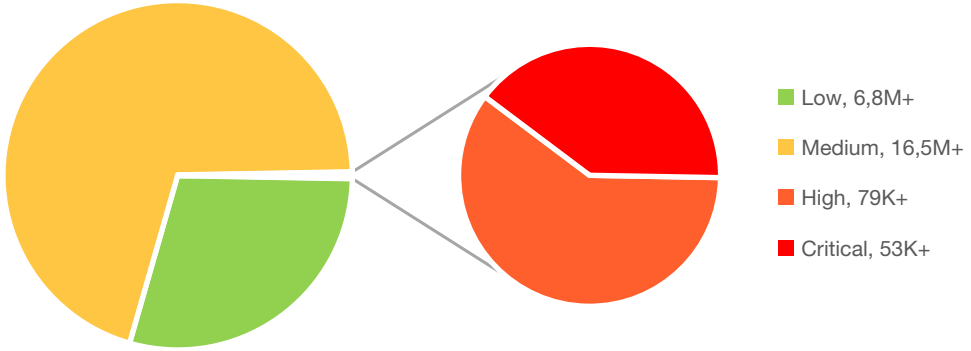


Figure 8. Level of alerts in Q4 2025

The vast majority, or **70%, of alerts are medium-level**, while 29% are low-level alerts related to system noise, false positives, configuration deficiencies or less serious cases.

Cyber incidents identified during the reporting period and recommended actions

Cyber incidents	Initial access	Recommended action
Password brute-force attacks 	Workstations connected to external networks, bypassing corporate security policies and devices exposed to the internet without a local firewall. This increases the vulnerability to automated attacks.	► Install local firewalls. ► Provide a VPN connection to the corporate network. ► Use strong, unique passwords and MFA.
Use of unwanted software in a corporate environment 	Unofficial activation tools, games, file-sharing software (BitTorrent), etc., may contain malware that threatens the integrity of the system and may compromise the system.	► Implement a software whitelist. ► Uninstall unauthorised apps and programs used for private purposes. ► Remove outdated / duplicate applications. ► Do not use software from non-NATO/EU manufacturers. ► Do not use multiple remote access tools at the same time
Malware Trojans 	Files downloaded from the internet	► Implement a software whitelist. ► Update your browsers regularly. ► Use browser extensions that block suspicious scripts. ► Educate and train employees on current cyber risks and cybersecurity.

Approximately 1% of all alerts are high-level (more than 79,000). These create a significant workload for the SOC team, as they are indicators of potentially dangerous attacks and require careful review.

The number of critical alerts (more than 53,000) quantitatively relatively small compared to the total volume, but **requires the greatest attention**.

The absolute number of critical and high-level alerts (more than 133,000), compared to Q3, has **increased almost fourfold**. This indicates persistent serious threats.

Within the CERT.LV SOC service, **8 cyber incidents were recorded** that had an impact on end devices or organisational infrastructure.

Practice shows that institutions and companies that have implemented and use CERT.LV SOC services are able to detect such threats much faster and mitigate them more effectively.

Cybersecurity threat hunting operations

Since 2022, when cybersecurity threat hunting was launched, by the end of Q4 2025, threat hunting operations have analysed in total:

- **~163 500** end devices (Q4 increase of ~1 500);
- in the ICT infrastructures of **more than 40** NCL subjects;
- **APT presence** in devices was identified in approximately **20%** of all analysed organisations.

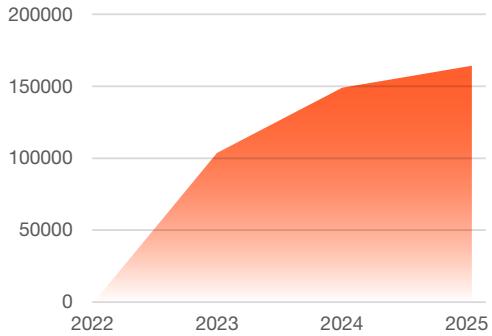


Figure 9. Dynamics of the volume of devices analysed during threat hunting operations (2022–2025)

This shows that Latvian organisations, including critical infrastructure operators, are a target for Russia, and that the CERT.LV services implemented, combined with local and international partnerships, make Latvia an increasingly inconvenient target, as attackers' activities are detected and mitigated more quickly, thereby achieving a deterrent effect.

Latvia and Canada continue to strengthen NATO cybersecurity capabilities

During the reporting period, at the beginning of November, Riga hosted the third four-day Threat Hunting Training Course on cyber threat detection, jointly led by Canadian and Latvian cybersecurity experts.

The objective of the training course was to support and strengthen NATO allies' capabilities in identifying potential threats. The training was organised in cooperation with the Ministry of Defence, CERT.LV and the Canadian Armed Forces Cyber Command. The training was attended by **33** representatives from **11** countries.

IT system security tests and phishing attack simulations

IT system security tests

Q4 2025 The CERT.LV team conducted **4** IT system security tests, during which a total of **24** vulnerabilities were identified, including **3** critical and **4** high-risk ones.

The purpose of security testing is to identify potential vulnerabilities, security threats and system deficiencies in order to prevent possible cyber attacks and data leaks.

Phishing attack simulation campaigns

During the reporting period, **6** phishing campaigns were carried out to train and enhance organisation employees' ability to identify potentially risky behaviour patterns, recognise and prevent cyber threats and information leakage. Total campaign audience: **1 800** persons.

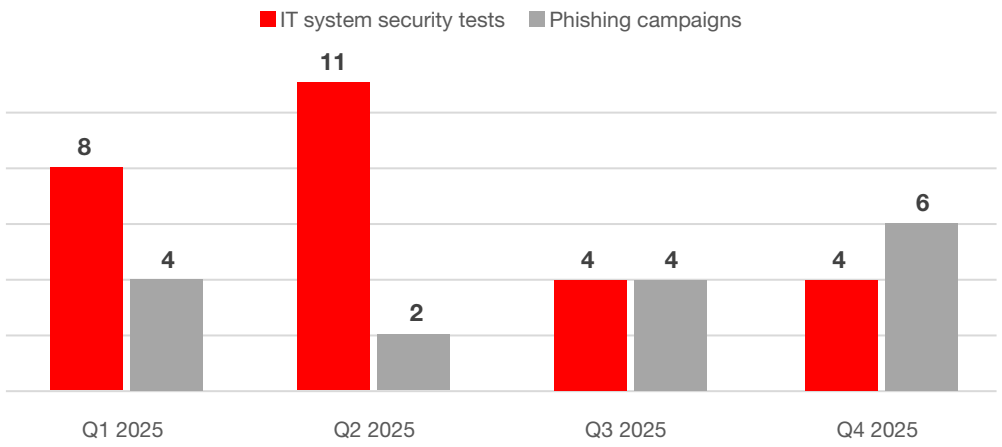


Figure 10. CVD platform: Number of vulnerability reports in Latvia

Vulnerability Reporting Platform (CVD)

The CVD platform is intended to facilitate cooperation between state and local government institutions and cybersecurity researchers and to improve the security of ICT resources.

Using the CVD platform, an institution can register information on all ICT resources it uses for which it wishes to receive reports on identified vulnerabilities. The platform provides a transparent and user-friendly interface where all received reports can be viewed, and communication with researchers and other involved parties can be maintained.

Total number of cases registered on the CVD platform as of the end of the reporting period (December 31, 2025):

- **148** security researchers (Q4 2025 increase of +16)
- **434** vulnerability reports (Q4 2025 increase of +60), including:
  - ✓ **262** client vulnerability reports processed by CERT.LV (Q4 2025 increase of +59)
  - **172** vulnerabilities reported for specific institutional programmes (Q4 2025 increase of +1)

View active institutional programmes here: **https://cvd.cert.lv/programs/all**

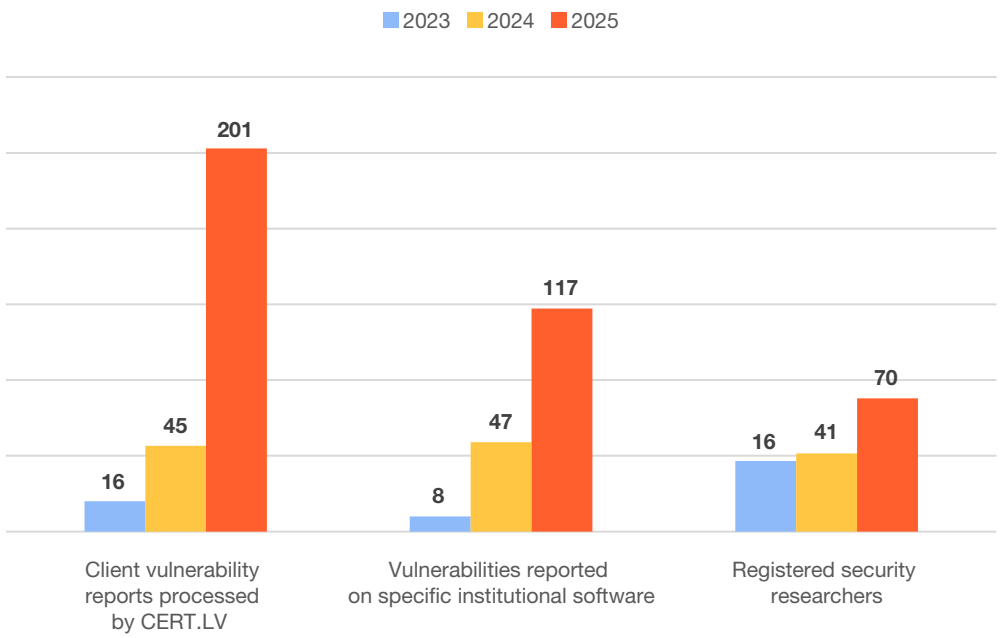


Figure 11. CVD: Number of vulnerability reports per year

CERT.LV offers a broad range of cybersecurity services that effectively protect the ICT infrastructure of organisations and bolster their cyber resilience. Protect and strengthen your cyberspace today using CERT.LV expertise, recommendations and services. More information on the website: CERT.LV

If you would like to receive a CERT.LV service, please write to us at cert@cert.lv

4. Strengthening cybersecurity through society-wide measures

- During the reporting period, in **70** events, CERT.LV experts educated **24,237** participants on cybersecurity, strengthening the knowledge, digital skills and cyber resilience of individual users and organisations.

Practical activities in public education

- Two new training tools were provided for state institutions, NCL subjects and members of the Cybersecurity Competence Community: the interactive material **"Business Continuity Challenge"** for crisis readiness testing and the escape room **"Ctrl + Alt + Escape[D]"**, which trains risk recognition through game-based principles. Projects co-financed by the European Union programme "Digital Europe".
- During the reporting period, every resident had the opportunity to assess their knowledge in a cybersecurity test developed as part of the public awareness campaign "Sniff out the scheme!" ("Ož pēc shēmas!"), organised by the Ministry of Defence and CERT.LV , promoting awareness of everyday digital risks. During the campaign, **6 025** respondents completed the test, while **8 300** started it.
- The platform kibertests.lv was launched to test and strengthen cybersecurity knowledge of residents and organisations. The test provides valuable recommendations and practical guidelines that help protect both personal and company data in everyday life, making the digital environment safer. The project is co-financed by the European Union programme "Digital Europe".
- On 9 December, the seminar **"Be safe!" ("Esi Drošs!")** took place, bringing together a total of **921** participants (in person and online).

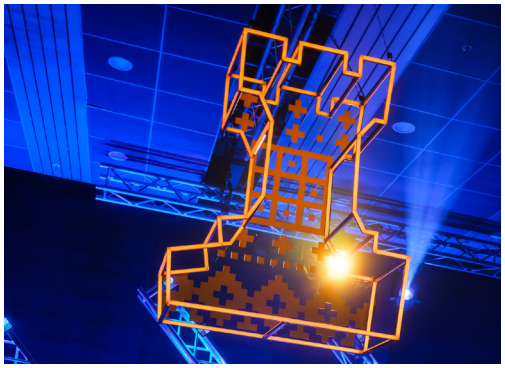
The most anticipated cybersecurity event in the Baltics was successfully held

On 29–30 October in Riga, the cybersecurity conference **"CyberChess 2025" (Kiberšahs 2025)** brought together more than **800** participants in person (including 62 speakers) and recorded more than **8 900** online views from at least **48** countries worldwide. Industry professionals, policymakers, researchers and industry representatives from the public, private and military sectors came together in one place, demonstrating that cybersecurity is a shared task and responsibility.

More than **200** participants from around the world took part in the CTF (Capture The Flag) competitions held as part of the conference. Three Latvian teams stood out with excellent results, winning prize places.

Organisers of the CyberChess 2025 conference: CERT.LV, the Ministry of Defence of the Republic of Latvia and the National Cybersecurity Centre, in cooperation with the ISACA Latvia Chapter, the Latvian Internet Association and the Institute of Mathematics and Computer Science of the University of Latvia.

Conference co-financing: The European Union, within the project of the Latvian National Coordination Centre (NCC-LV) of the European Cybersecurity Competence Centre.



CERT.LV's mission is to promote cybersecurity in Latvia.

The main tasks of CERT.LV are to maintain and update information on cybersecurity threats, provide support to state institutions in the field of cybersecurity, assist in resolving cybersecurity incidents for any natural or legal person if the incident involves a Latvian IP address or a .LV domain, as well as to organise informational and educational events for government employees, IT security professionals, and other interested parties.

The report includes publicly available information and does not contain any restricted information. This report is for information only.

Contact CERT.LV:

Phone: +371 67085888

E-mail: cert@cert.lv

Website: www.cert.lv

Follow CERT.LV news on:

@cert.lv