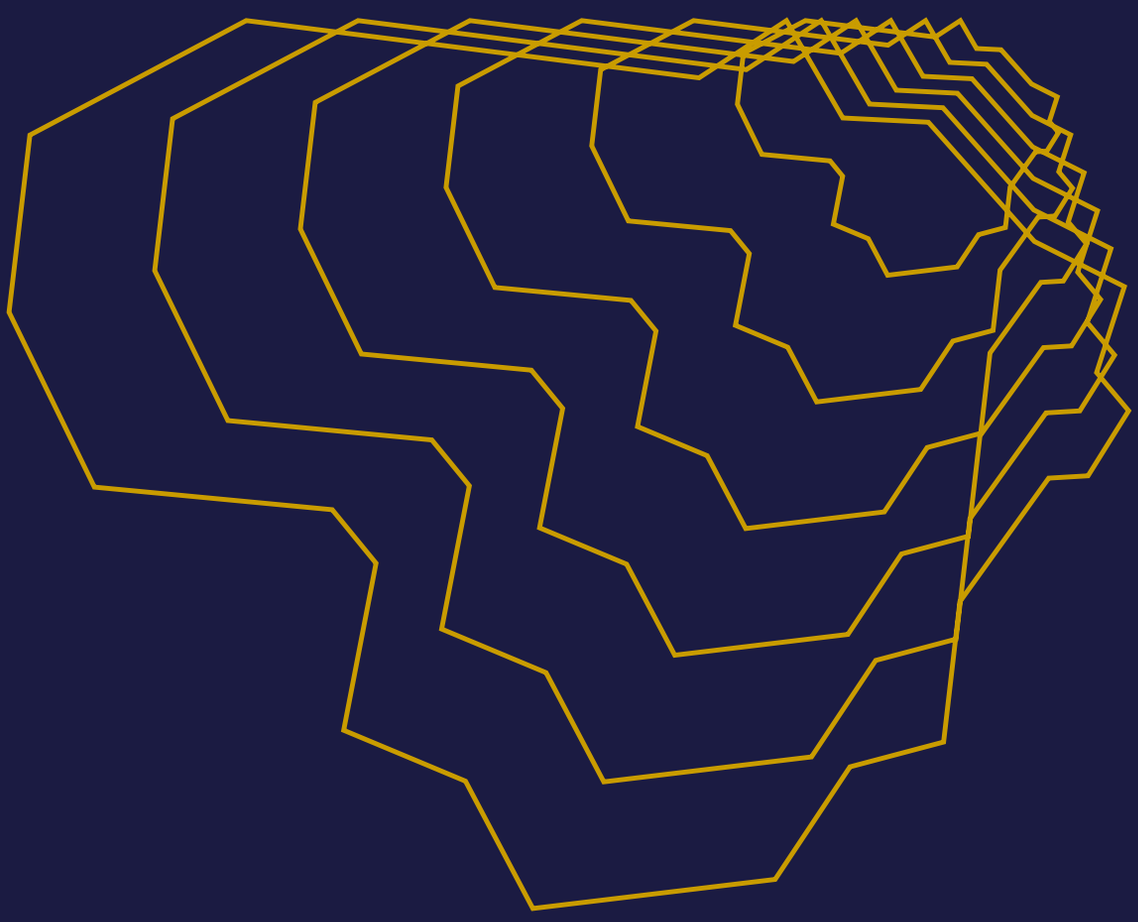
MINISTRY OF NATIONAL DEFENCE
OF THE REPUBLIC OF LITHUANIA

OVERVIEW OF THE CYBERSECURITY STATUS IN LITHUANIA: KEY INFORMATION



2025

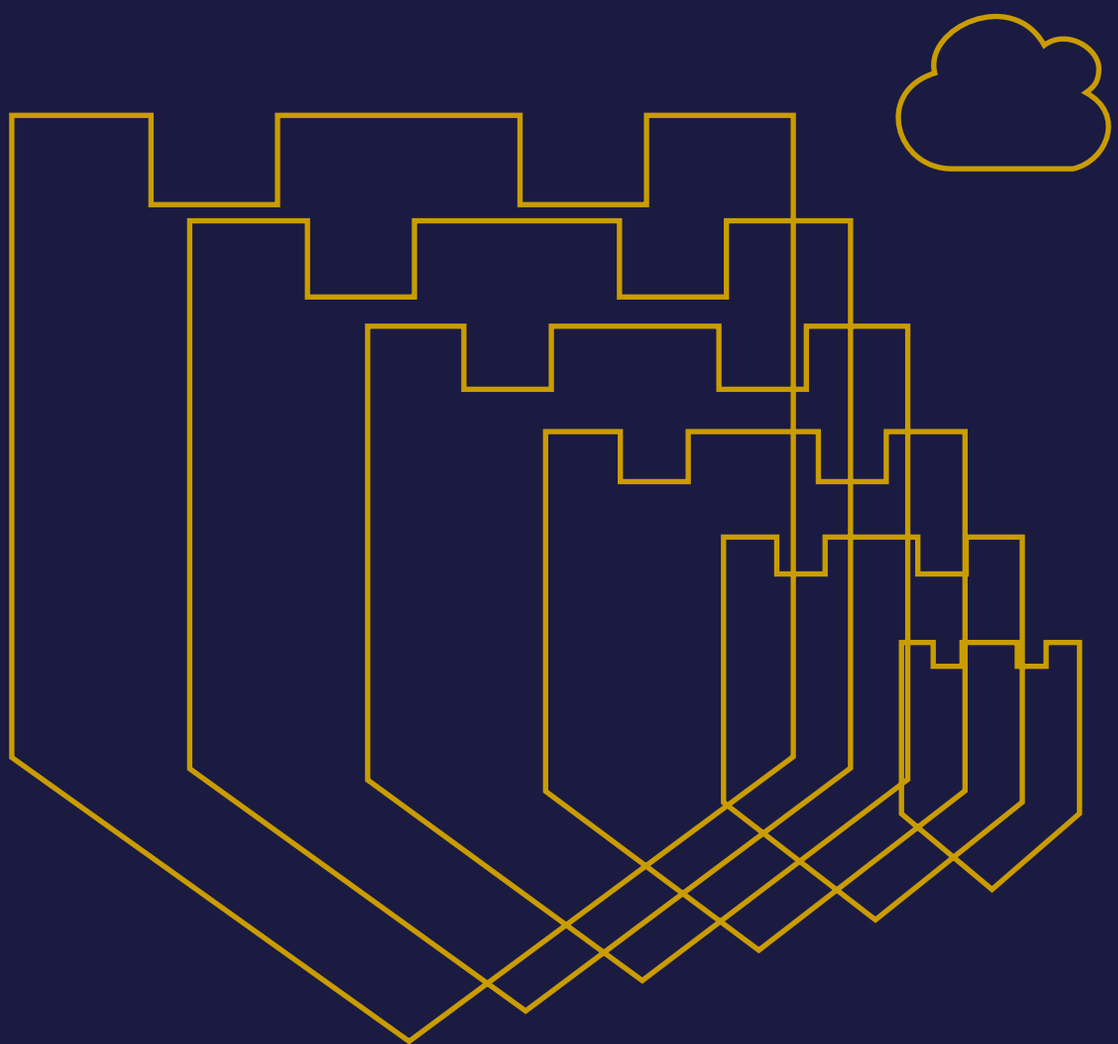
OVERVIEW OF THE CYBERSECURITY STATUS IN LITHUANIA: KEY INFORMATION

2025

Vilnius

01

Foreword



Foreword

Robertas Kaunas,
Minister of National Defence

With many years of experience in the IT industry, I am aware that cyberspace is a battleground. It is where state-sponsored groups, organised criminals, and opportunistic, malicious actors operate. Attacks against Lithuania and our allies are not incidental — they are deliberate, targeted, persistent and integrated into a broader hybrid warfare strategy. Attacks on critical infrastructure, efforts to discredit institutions, and attempts to polarise society occur simultaneously across multiple channels.

In 2025, a total of 2,888 cyber incidents were recorded, marking a 25% decrease compared to 2024. The number of cybercrimes decreased by 28%, and its detection rate increased by 10.5%. While these are encouraging signs, the registered figures do not reflect the full picture, as some incidents continue to be unreported due to an insufficiently developed reporting culture.

Threats are increasingly targeting people with access to systems, rather than the systems themselves. Incidents involving social engineering accounted for the largest share of all recorded cases in 2025. Fraud remains the predominant form of cybercrime — accounting for 44% of all cybercrimes — and financial losses reach tens of millions of euros.

The National Cyber Security Centre under the Ministry of National Defence responds to cyber threats systematically and at scale. In 2025, the DNS firewall blocked malicious activity an average of 50,000 times per day — nearly five times as often as in 2024. Over the course of the year, approximately 13 million fraudulent calls and nearly 6 million spoofed short text messages (SMS) were blocked.

Vulnerabilities among entities operating in sectors of high criticality and other critical sectors remain a significant source of risk, as insufficient cybersecurity measures may provide access paths to essential systems. Of the 153 information systems assessed by the National Cyber Security Centre, 64% were found to be vulnerable. This means that strengthening resilience must become a continuous process, rather than a periodic compliance check.

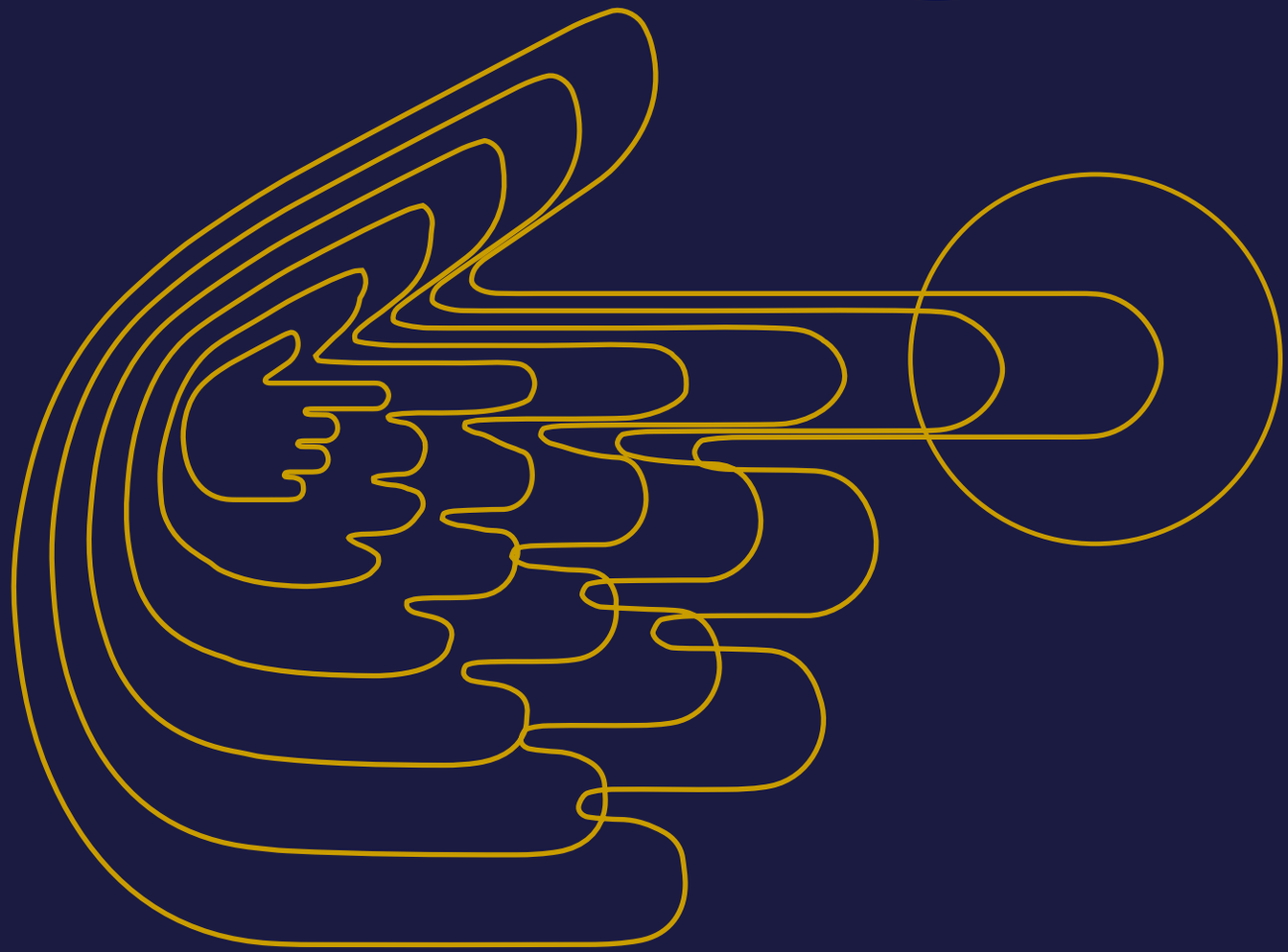
That is precisely why we are expanding the scope of responsibility. In 2025, the Registry of Cybersecurity Entities included 1,443 organisations, and the scope of mandatory requirements had increased several-fold. Organisations providing critical services are beginning to implement specific organisational and technical standards — an important step in the daily process, but not an end in itself.

Artificial intelligence is changing the threat landscape faster than we can adapt. Deepfakes, automated attacks, and sophisticated intrusion tools are becoming accessible to everyone. This only confirms once again: investments in people and technology are vital. The decisions we make today regarding system architecture, data management, and workforce capabilities will directly determine the vulnerability landscape tomorrow.

Cybersecurity is not just an IT issue — it is a matter of national governance. Let us address it together.

02

Essential Tasks, Trends and Statistics



Summary

The scale, speed, and complexity of cyber threats continue to increase, while traditional defence models struggle to adapt at the same pace. Technological advancements, the development of artificial intelligence (AI), and growing dependence on digital services not only create new opportunities but also expand the cyberattack surface, reduce the time available to detect and contain incidents, and increase their impact. Therefore, no organisation or state can effectively ensure security without the support of partners. Cooperation among public institutions, businesses, academia, and international partners is a prerequisite for strengthening cyber resilience.

The National Cybersecurity Status Report was prepared by the Ministry of National Defence (MoD), based on data and insights covering the period from 1 January to 31 December 2025. The Report draws on contributions from key partners within Lithuania's cybersecurity ecosystem: the National Cyber Security Centre under the Ministry of National Defence (NCSC), the Lithuanian Police, the State Data Protection Inspectorate (SDPI), the Communications Regulatory Authority (RRT), and the Strategic Communications Department of the Lithuanian Armed Forces (SCD). The Report presents the key threats, indicators, trends and response measures identified within the areas of responsibility of these institutions. It covers topics ranging from incident management and cybercrime investigations to reliability of electronic communications, personal data protection and monitoring of information threats. The Report provides a clear and comprehensive overview of Lithuania's cybersecurity landscape.

It is intended for the public, organisational leaders, experts, and decision-makers seeking to better understand risks, strengthen resilience, and make informed decisions. Information relating to 2026 is indicated in the footnotes

MoD has been strengthening Lithuania's cyber resilience and preparedness for next-generation threats

In developing its cybersecurity policy, the MoD, in partnership with other Lithuanian institutions, strengthened interinstitutional cooperation to enhance public awareness and improve preparedness to identify and prevent cyber threats. Cooperation agreements have been signed with the Ministry of the Interior, the Ministry of Education, Science and Sports, the Ministry of Culture, and the Ministry of Health.

As part of the implementation of the MoD's National Cybersecurity Development Program, comprehensive upgrades involved updating cybersecurity infrastructure, organising capacity-building and training activities, conducting public awareness initiatives, and reviewing relevant legislation. To prepare for the quantum era and ensure a timely transition to post-quantum cryptography (PQC), draft guidelines were developed to help organisations manage the transition process.

The MoD continued to play an active role in shaping the European Union's (EU) cybersecurity policy. In 2025, the MoD participated extensively in discussions on proposed amendments to EU cybersecurity legislation, including the NIS2 Directive, as well as new legislative initiatives, such as the Digital Omnibus. Together with other EU countries, Lithuania also contributed to discussions on the new EU cyber crisis management framework and participated in cyber crisis management exercises.

In 2025, international cybersecurity cooperation was actively fostered. Consultations continued with Poland, Latvia, Moldova, the United States, and partners in the Indo-Pacific region, while new cooperation initiatives were launched with Finland and Canada.

In 2026, particular attention will be given to supporting organisations in their transition to PQC, the management of the PESCO Cyber Rapid Response Teams (CRRTs) and Mutual Assistance in Cyber Security project and the participation of CRRTs in military missions and operations under the EU Common Security and Defence Policy (CSDP), as well as in missions in EU partner countries. In 2026, significant attention will be devoted to preparations for Lithuania's Presidency of the Council of the EU.

According to the NCSC, a 25% decrease in cyber incidents indicates progress, but the maturity of organizations remains uneven

In 2025, a total of 2,888 cyber incidents were recorded in Lithuania, representing a 25% decrease compared to 2024. This was due to both the NCSC's more effective implementation of preventive measures, including the blocking of more than 70,000 malicious domains, and growing cybersecurity awareness among organisations. On the other hand, some incidents may not have been reported due to differing interpretations of legal regulations or a lack of expertise in identifying cyber incidents.

The majority of incidents were minor or near-misses. Only 19 significant incidents were recorded. This reflects the growing incident management capabilities of the NCSC and other organisations, while indicating that cyber threats are constantly expanding.

Digital infrastructure (e.g., cloud, hosting, and information and communications technology (ICT) service providers' systems) is becoming both a primary target for attacks and a platform for launching further cyberattacks. The majority of cyber incidents (2,118) involved the infrastructure of foreign hosting service providers used to publish and distribute malicious content.

Another trend emerged in 2025: nearly twice as many cyber incidents occurred in the information systems of Lithuanian legal entities (from 155 incidents in 2024 to 280 incidents in 2025). This indicates that significant risks originate within organisations themselves. These incidents typically stem from human factors: a lack of employee vigilance and insufficient cybersecurity awareness.

In 2025, an increasing number of cyber incidents (267) was recorded in Lithuania's digital infrastructure. They were related to service disruptions, attempted intrusions, and various operational disruptions.

It is worth noting that the nature of cyber threats remains largely unchanged — more than 54% of all incidents are related to social engineering. On the other hand, the number of such incidents in 2025 was nearly one-third lower than in 2024. Even as technological resilience grows, the greatest risk remains linked to human behaviour, vigilance, and the ability to recognise fraudulent schemes.

Account takeover remains the primary method of intrusion attacks. The NCSC uncovered over 106,000 leaked credentials across public and restricted information sources and notified 221 organisations, issuing nearly 3,000 notifications (2,000 in 2024). This indicates that data leaks continue to serve as the foundation for further attacks. The main causes of credential leakage remain infostealer malware, as well as human error. In response to the ever-growing threat, the NCSC has automated notifications regarding leaked credentials and has begun preparing sector-specific cyber threat reports.

Vulnerabilities identified by the NCSC in networks and information systems remain a significant concern. Websites, web applications, and network devices remain among the most common targets of cyber threats, and the vulnerabilities identified indicate that some organisations still do not adequately protect publicly accessible systems or promptly address known vulnerabilities.

Changes in the cybersecurity ecosystem in 2025: as many as 1,443 organisations were included in the Register of Cybersecurity Entities, and the scope of the NCSC's oversight increased nearly fivefold. Work has begun on the development of a national modular Security Operations Centre (SOC) system, laying the foundation for faster and more coordinated incident response at the national level. Practical guidance was developed in key areas of cy-

bersecurity, including the responsible use of AI, third-party risk management, and cyber risk management. Interinstitutional cooperation with the financial sector and law enforcement authorities is being developed to facilitate faster information sharing and more effective responses to threats.

Looking ahead to 2026, it is likely that the main threat vectors will remain unchanged, but their scale and complexity will continue to grow. Due to the use of AI, cyberattacks will become faster and more convincing, and dependence on supply chains will remain one of the main systemic vulnerabilities.

According to Lithuanian Police data, cybercrime declined in 2025, but fraud continues to evolve and remains the primary threat

In 2025, the number of criminal offences recorded in Lithuania decreased by 7%, while cybercrime declined by 28% compared to 2024. Over the past five years, the crime rate has remained stable, with no increase in risk observed.

Fraud (44%) and offences targeting information systems (21%) continued to account for the largest share of cybercrime. Although the number of fraud offences stabilised in 2025, recording a 7% decrease and marking the first decline after five consecutive years of growth, the financial impact of fraud remains significant. According to data from financial market participants, attempts were made to fraudulently obtain €58.8 million, more than half of which were thwarted. However, losses incurred by the public amounted to approximately €20.5 million, slightly higher than in 2024 (by about €0.5 million). This was driven by the targeted exploitation of vulnerable social groups and the trade in leaked data, posing a significant threat to international security.

The trend persists, with fraud cases primarily aimed at obtaining financial gain (81%, 16% higher than in 2024) and targeting online banking users (76%, also 16% higher than in 2024). There is a growing risk that victims may be exploited as unwitting accomplices to crimes and for other purposes, such as carrying out hybrid attacks.

In 2025, the prevalence of fraudulent calls and website spoofing increased significantly. Although the number of fraudulent calls decreased in the second half of 2025 due to the implementation of countermeasures and blocking measures, the risk posed by them remains high, driven by organised, international criminal networks and increasingly aggressive criminal methods. Website spoofing, which began spreading systematically in late 2024,

remains dynamic and may become one of the dominant methods of fraud as criminals adapt to preventive measures and seek new ways to reach victims, bypass security controls, and compromise accounts or financial data.

In 2025, the number of criminal offences targeting the security of electronic data and information systems increased by approximately 10.1%, but their severity remained low. The greatest risk of cybercrime stems from unauthorised access to information systems, but the trend remains stable.

In Lithuania, unlike in other EU countries, ransomware and distributed denial-of-service (DDoS) attacks have been sporadic rather than systematic, accounting for less than 1% of all cybercrimes.

Although the police have not yet observed the widespread use of AI in criminal activities, its use for criminal purposes is increasing and poses long-term challenges for law enforcement. At the same time, the police are strengthening their technological capabilities by implementing an advanced analytical tool designed to analyse data and investigate complex criminal offences.

As trends related to fraud, AI-enabled crime, and ideologically motivated cyberattacks persist, particularly those linked to the geopolitical situation and hybrid threats, the ability of law enforcement to strengthen capabilities and ensure effective cooperation will be critical. Equally important will be systematic solutions aimed at adapting legislation to a rapidly evolving technological environment.

According to SDPI, 29% of personal data breaches (PDB) in Lithuania in 2025 were caused by cyber incidents

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

In 2025, the SDPI received 223 notifications of PDBs, representing an 18% decrease compared to 2024. According to the SDPI, this decline may have been positively influenced by the entry into force of amendments to the Law on Cyber Security, the expanded list of cybersecurity entities, the clear regulation of technical and organisational measures, and the SDPI's regular awareness-raising activities.

In 2025, 29% of PDBs were caused by cyber incidents; however, these breaches affected as many as 57% of all affected data subjects (713,644), accounting for more than half of all individuals affected by PDBs in 2025.

An analysis of notifications of PDBs related to cyber incidents revealed that 45% of PDBs resulted from unauthorised access to IT systems by malicious actors, 26% resulted from social engineering and phishing attacks, 16% resulted from ransomware attacks. The causes of 6% of all PDBs notifications received in 2025 could not be determined. This suggests that, following a cyber incident, data controllers are unable to properly conduct an investigation and identify its causes, which could help prevent such attacks in the future.

Cases assessed by the SDPI in 2025 revealed that PDBs affecting Lithuanian residents, both in Lithuania and elsewhere in Europe, exposed systemic weaknesses: human error, supply chain vulnerabilities, and insufficient oversight of third parties. This highlighted the need to strengthen employee competencies, internal controls, and the maturity of risk and incident management, as well as to evaluate AI tools in use more rigorously.

Following the SDPI's assessment of 2025 data and prevailing global and domestic trends, it is evident that social engineering and phishing attacks continue to succeed due to insufficient employee awareness of social engineering indicators, the lack of additional authentication measures enabling the misuse of compromised credentials, supply chain vulnerabilities, and insufficient oversight of third parties.

Based on the SDPI's experience in assessing PDBs notifications received in 2025, it is reasonable to predict that, in 2026, the challenges associated with the use of AI in relation to personal data protection will remain relevant and require consistent attention from both supervisory authorities and organisations. In 2026, the SDPI will continue its public awareness activities and efforts to strengthen public understanding of cyber fraud and help individuals recognise threats in a timely manner in order to protect themselves more effectively.

RRT measures to combat fraud and harmful online content have strengthened cybersecurity, but new risks have emerged

In 2025, Lithuania's electronic communications infrastructure remained stable. No major disruptions were recorded, and services were typically restored within approximately two hours. However, new risks emerged: harmful radio interference originating in the Kaliningrad region affected aircraft and maritime navigation systems, mobile network base stations, and border areas. The intensification of harmful radio interference at the end of 2025 indicated that interference in the Baltic region is becoming a long-term and systemic challenge that requires continued attention at both the EU and international levels.

The scale of telephone fraud continued to grow rapidly in 2025 — although millions of fraudulent calls (63% more than in 2024) and spoofed SMSs (nearly 80% more than in 2024) were blocked, this indicates not only more effective protection measures but also the increasing intensity of the threat itself. Fraud schemes are becoming increasingly adaptive, the number of spoofed Lithuanian phone numbers is rising, and new social engineering techniques are constantly being employed; therefore, it is essential to strengthen the regulatory and operational responses so that measures are effective not only in reacting to incidents, but also in preventing them.

The use of electronic identification and qualified electronic signatures has become widespread in Lithuania, and the reliability of these tools is directly linked to trust in the digital environment. In 2025, decisions made by RRT in this area increased the availability of such services and expanded choice within the market.

In implementing the Digital Services Act (DSA) and its provisions into national legislation, Lithuania distinguished itself among other EU countries through the active use of mechanisms for the removal of illegal content. During the first half of 2025, Lithuanian authorities submitted 480 notices to very large online platforms (VLOPs) (EU total: 2,700). In addition, approximately 6 million links to illegal content were removed following reports submitted by Lithuania's trusted flaggers, thereby reducing users' exposure to harmful content online.

Efforts to prevent the dissemination of illegal content and content harmful to minors online highlighted growing risks in 2025. Lithuania's "Clean Internet" hotline service received more than 3,500 reports (nearly 62% more than in 2024), of which more than 2,200 were confirmed. The scale of cyberbullying grew particularly rapidly — the number of confirmed cases in 2025 increased approximately three times compared with 2024, and by more than five times over the past three years. Reports of online child sexual abuse material (CSAM) also increased by 18%, with the majority of such content hosted on servers located outside of Lithuania. The effectiveness of efforts to combat harmful online content depends directly on prompt cooperation between Lithuanian institutions and international partners.

To strengthen society's ability to recognise cyber threats and use digital services safely, RRT continued the "No One Left Behind" project in 2025. The project brought together hundreds of partners across Lithuania, while digital literacy training reached tens of thousands of residents, particularly elderly adults.

Looking ahead to 2026, RRT will seek to consistently strengthen the security and reliability of electronic communications networks and digital services, focusing primarily on combating online fraud and fostering a safer digital environment.

According to the SCD data, the number of cases of hostile information activities increased in Lithuania in 2025

In 2025, the SCD identified 3,707 cases of hostile information activities involving the dissemination of misleading or false information targeting Lithuania or its partners (NATO, the EU). This increase was associated with intensified Belarusian activity in the information environment and Russia's systematic actions targeting NATO and the EU.

Defence and security topics have remained dominant in the hostile information environment for several years. In 2025, they accounted for 70% of all identified cases of hostile information activities targeting Lithuania or its partners. Additionally, particular attention was given to the Baltic Sea and Kaliningrad regions. Decisions related to Lithuania's defence policy were a key target of hostile states, with particular emphasis placed on efforts to strengthen border defence along its borders with Russia and Belarus.

In 2025, a noticeable increase occurred in the Belarusian regime's information pressure against Lithuania, aimed at convincing both domestic and international audiences that Lithuania's foreign policy is irrational, aggressive toward Belarus, and harmful to Lithuanian citizens. The most active channels for spreading propaganda remained state-controlled and regime-controlled media outlets, as well as social media platforms, primarily Telegram.

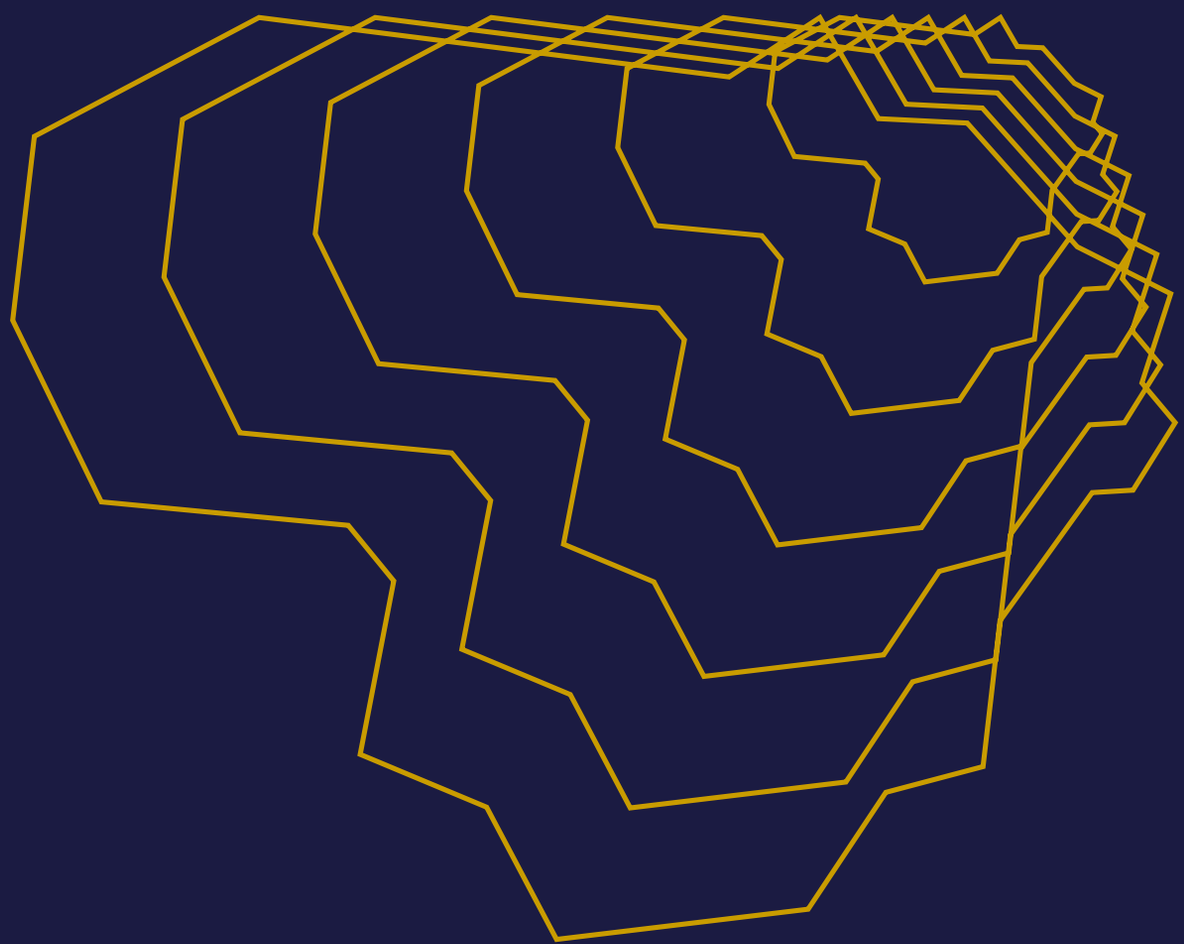
During the same period, AI emerged as a threat within the area of responsibility of the SCD. It has been used in cyberattacks, social engineering and fraud schemes, as well as in information and psychological operations. AI enables significantly larger-scale hostile campaigns, faster narrative adaptation, and a higher level of personalisation and obfuscation. In 2026, to help strengthen society's resilience to information threats, the SCD will continue its public awareness activities and share its insights with the media and the public.

Strengthened interinstitutional cooperation in response to cyber threats

A growing trend shows that certain cyber threats, particularly fraud based on social engineering techniques, now span multiple domains simultaneously and cannot be effectively addressed through the efforts of individual institutions alone. Such threats simultaneously affect law enforcement, financial systems, electronic communications, and cybersecurity, undermining the interests of both individuals and organisations. In this context, rapid information sharing, coordinated action, and aligned preventive measures provide the greatest value. In light of this, on 27 March 2025, the Bank of Lithuania, the Lithuanian Police, the Prosecutor General's Office of the Republic of Lithuania, the NCSC, the CRA, and the Centre of Excellence in Anti-Money Laundering signed a Memorandum of Cooperation to combat fraud in the digital space. The Memorandum aims to pool the capabilities of these institutions to jointly fight fraud in the digital space, ensuring rapid information exchange, coordinated responses, joint preventive measures, and more effective public warnings about threats.

In addition, on 28 July 2025, the NCSC and the Bank of Lithuania signed a cooperation agreement on the exchange of information related to cyber incidents in the financial sector. The Bank of Lithuania, as the financial market regulator, was the first to join the NCSC's National Cyber Incident Management Platform. The Bank of Lithuania gained the ability to exchange information on cyber incidents and cyber threats automatically and in real time, enabling faster responses to threats and closer cross-sector cooperation.

Experience from 2025 shows that the most effective response to cyber threats is not isolated responses, but continuous cooperation among government agencies, regulators, law enforcement, and critical sectors. Such cooperation accelerates not only incident response but also strengthens Lithuania's overall cyber resilience.



OVERVIEW OF THE CYBERSECURITY STATUS IN LITHUANIA: KEY INFORMATION 2025

Published by the Ministry of National Defence of the Republic of Lithuania
Totorių St. 25, LT-01121 Vilnius, www.kam.lt 20/05/2026. Order No. GL-413

Layout by the Visual Information Division of the General Affairs Department,
Ministry of National Defence Totorių St. 25, LT-01121 Vilnius

Bibliographic information of the publication is available in
the National Bibliography Data Bank
of the Martynas Mažvydas National Library of Lithuania.

ISSN 2783-7017