



NATIONAL
SECURITY
AUTHORITY

ANNUAL REPORT ON CYBERSECURITY OF THE SLOVAK REPUBLIC 2024





NATIONAL
SECURITY
AUTHORITY

ANNUAL REPORT ON CYBERSECURITY OF THE SLOVAK REPUBLIC 2024

CONTENTS

1	THREAT OVERVIEW	4
1.1	Global factors affecting cybersecurity	4
1.2	The most significant threats in the Slovak Republic in 2024	6
1.3	Threat actors	8
2	STATISTICAL OVERVIEW OF INCIDENTS	10
2.1	Basic overview	10
2.2	Incidents by sector	12
3	THE STATE OF CYBERSECURITY	13
3.1	Overall view	13
3.2	Audits and self-assessments	14
3.3	State supervision	15
3.4	Banking sector	16
3.5	Digital infrastructure sector	16
3.6	Electronic communications sector	17
3.7	Energy sector	17
3.8	Public administration sector	18
3.9	Water and atmosphere sector	19
3.10	Health sector	19
3.11	Assessment of the state of cybersecurity by central authorities	20
4	ACTIVITIES AND ACTIONS OF THE NSA	23
4.1	National legislation	23
4.2	European Unio	24
4.3	OSCE	25
4.4	NATO	26
4.5	Regional cooperation	27
4.6	Bilateral relations	28
4.7	Issuing warnings and bulletins	29
4.8	CyberGame	29
4.9	Awareness raising for the general public	29
4.10	Activities of the CSCCC	30

1 THREAT OVERVIEW

1.1 GLOBAL FACTORS AFFECTING CYBERSECURITY

1.1.1 Military conflicts

The key geopolitical factors affecting Slovak cyberspace include ongoing military conflicts, especially Russia's aggression against Ukraine, which has long had a major impact on European security. In this military conflict, cyber operations are a significant element influencing events on the battlefield, intelligence and cybersecurity of both sides. The experience of the conflict in the field of cybersecurity and defence is already a valuable lesson for the whole world.

China's increasing assertiveness and its efforts to expand its influence beyond the Southeast Asian region pose a challenge to both cybersecurity and digital sovereignty. However, developments in the Middle East - the ongoing Israeli-Palestinian conflict and the ambitions of other actors in the region (notably Iran) - cannot be overlooked.

1.1.2 Elections abroad

The year 2024 was characterised by high levels of electoral activity, with elections taking place in seven of the world's ten most populous countries, including the United States (US). European Parliament elections were also held in the Member States of the European Union from 6 to 9 June 2024. Cyber-attacks and the spread of disinformation are an increasingly common tool for influencing both public opinion and the outcome of elections. Neglecting cybersecurity in these cases can have far-reaching consequences not only for the internal political development of individual states, but also for the stability and direction of entire regions.

The European Parliament elections posed a particular challenge in terms of cybersecurity. Its specificity lies in the parallel voting in the 27 EU Member States, with each country having a different technological infrastructure and level of protection. This fragmentation creates differences in the vulnerability of electoral systems, increasing the risk of disruption. Potential incidents can undermine confidence in the legitimacy of elected representatives and thus undermine the credibility of the European Parliament as a whole.

Among the most significant threats that accompanied the elections abroad was the systematic influence of public opinion through disinformation campaigns. The campaigns were often aimed at reinforcing preferences for particular candidates or political entities. They used sophisticated tools such as fake social media accounts, automated bots, targeted content and algorithmic amplification of polarising themes. Their aim was not only to influence the election result, but also to deepen social divisions and reduce citizens' trust in the democratic electoral process itself.

In parallel, direct cyber-attacks targeting multiple levels of electoral infrastructures were also taking place, targeting national electoral systems, voter databases, as well as the servers of political parties, candidates and institutions involved in the organisation and evaluation of elections. Particularly risky were the attempts to compromise systems directly related to the technical security of elections in some European

Union countries, which could compromise not only the conduct but also the overall results of the European Parliament elections.

Equally important was the third level of threats - the misuse of the human factor. In many cases, attackers sought to gain access to sensitive information by compromising the personal accounts of individuals who played key roles in election campaigns or in the organisation of voting. Information obtained in this way could subsequently be used to blackmail, discredit or manipulate the decision-making of these individuals.

1.1.3 CrowdStrike

In July 2024, there was a major outage of CrowdStrike's Falcon Sensor security software, which had a significant impact on technology infrastructure across various sectors around the world. Although this is software that is unfamiliar to most mainstream users, its importance in the cybersecurity field is fundamental. It is used on millions of devices, often without the knowledge of the users themselves, who are unaware that this 'antivirus' is running in the background of their systems.

Falcon Sensor is used for real-time malware and behaviour detection and is primarily implemented in corporate and government systems. On July 19 2024, CrowdStrike released a routine update called Rapid Response Content, which was intended to improve the sensors' ability to respond to new threats within the Windows operating system. However, a bug in this update caused millions of computers worldwide to go into a critical 'Blue Screen of Death' (BSOD) state, rendering them unusable.

This incident is a textbook example of a so-called cascading failure - a situation in which a technical problem in one component leads to a chain of failures in many linked systems. Only devices with Falcon Sensor version 7.11 and higher that received the update in a short window of time between 04:09 and 05:27 UTC were affected. After the bug was fixed, CrowdStrike issued a patch update, but by that time over 8.5 million devices were already affected.

The consequences were immediate and global. In the US, more than 3,000 flights were cancelled and another 11,000 were delayed. Slovakia was also affected by the outage - Milan Rastislav Štefánik Airport in Bratislava experienced a check-in system failure. In the healthcare sector, a number of interventions were suspended or postponed, which shows the degree of dependence of this infrastructure on the reliable functioning of IT systems. Financial institutions faced delays in transactions and payouts, media such as Sky News reported outages.

One of the most interesting cases that arose during the CrowdStrike outage was a wave of phishing attacks targeting clients in Latin America. Hackers tried to exploit a vulnerability created by the outage and sent out emails with infected attachments pretending to be official announcements from CrowdStrike. This type of attack was all the more dangerous because it targeted people who were unaware of the technical details of the outage.

1. 1. 4 Development of artificial intelligence

In recent years, we have witnessed a significant increase in the sophistication of cyber attacks, largely due to the integration of artificial intelligence (AI) into the arsenal of cyber criminals. Recent studies and incidents point to the fact that AI allows attackers to create extremely convincing and personalised phishing campaigns that are difficult to detect even for experienced users.

AI models have improved their skills in persuasiveness and deception compared to previous years. Whereas in the past AI models needed human assistance to achieve performance comparable to human experts, current models can generate highly effective phishing emails on their own. These advances highlight the rapid evolution of AI technologies and their potential misuse in cyberattacks.

1. 2 THE MOST SIGNIFICANT THREATS IN THE SLOVAK REPUBLIC IN 2024

1. 2. 1 Social engineering

There was a slight increase in the number of reported incidents in the first quarter of 2024 compared to the previous year. The highest number of incidents continued to be related to the acquisition of information, through the use of social engineering. Phishing attacks were the most prevalent type of malicious activity. Several phishing campaigns targeting employees of entities in the public administration sector were carried out during the reporting period. During these campaigns, attackers successfully compromised a number of email accounts, which were subsequently exploited to further disseminate phishing messages. Especially dangerous were the campaigns disseminated from compromised email accounts with .sk and .cz domains. The analysis showed that these attacks mainly affected the systems of specific providers, indicating intrusions into their infrastructure.

During the period in question, phishing campaigns targeting the general public were also recorded, with the likely intention of the attackers being to obtain personal and sensitive data from victims in order to misuse it in further malicious activities or to steal funds from bank accounts. The large-scale campaigns exploited, among others, the identity of the airport using the theme of selling luggage, but also the identity of the telecommunications company or streaming service provider.

In the context of global trends, one of the biggest cyber threats was ransomware. In the past period, a number of both operators of essential services and private sector organisations have fallen victim to this type of malicious activity. Ransomware tools from the LockBit 3.0 or RansomHub 'family' have often been used in attacks.

Among the various types of techniques, attackers also used malwaretisetment, i.e. spreading malicious code by means of trustworthy advertisements on legitimate websites. Several campaigns have been reported through which malware programmed to steal victims' data has been distributed. One of the cases involved the public administration sector and the campaign was also conducted using Slovak compromised accounts.

The upward trend in reported cybersecurity incidents has persisted, particularly in the area of information extraction, mainly through social engineering, phishing and smishing (SMS). Users of public administration information systems were regular targets of phishing campaigns to compromise email accounts. In the second quarter of

2024, the NSA noted an attempt to spoof a password change on a fraudulent email client website.

Fake SMSs were sent out with information about the expiry date of the vignettes, which redirected the recipients to a fake payment portal. On the Bazos.sk platform, scams continued, where attackers sent fraudulent emails to advertisers with fake instructions for courier services in an attempt to obtain payment card details. There has also been an increase in bogus phone calls in which fraudsters impersonate the police or Europol and intimidate victims by suggesting they have broken the law.

Other campaigns focused on the misuse of the identity of the slovensko.sk portal. In this case, victims were lured with fake messages about tax refunds or speeding fines. The attackers' goal was to obtain login details. In other cases, emails were sent out mimicking communications from energy suppliers. These contained attachments with malware such as the REMCOS infostealer, which is designed to steal sensitive data. Attackers also registered domains that resembled official government websites, such as 'govenment.sk' or 'vladagov.sk'. These domains were exploited to send phishing emails, and at certain stages of the attack, the attackers modified DNS records to mimic legitimate Govnet sites. In order to address this situation, there was a need to put in place controls to prevent the registration of domains mimicking the names of state institutions.

1.2.2 Unavailability of services and DDoS attacks

The prediction of possible cyber incidents during the European Parliament elections has come true. The experienced a large-scale Distributed Denial of Service (DDoS) attack on a major public sector website which was briefly unavailable.

Hacktivist groups launched a wave of DDoS attacks on the banking and public administration sectors in the aftermath of the attempted assassination of the Slovak Prime Minister. The aim of such attacks is usually to make frequently used products and services unavailable.

Europol confirmed the compromise of the Expert Platform Portal (EPE). This event had an impact on the Slovak Republic institutions and their users who participate in Europol activities on behalf of the Slovak Republic.

Slovakia has also faced a number of major cyber incidents that have highlighted the growing risks and vulnerabilities in various sectors. Among the most serious was the compromise of a water company, where attackers exploited a vulnerability in the ESXi platform. Similarly, the system of a social care facility for the elderly was compromised, with a ransomware attack disrupting its operations.

1.2.3 Bomb threats

Slovakia has long been the scene of anonymous bomb threats. Threats are mostly aimed at school facilities, courts, towns and villages, airports and similar institutions. They are typically reported by telephone or email, and law enforcement authorities have often succeeded in tracking down the perpetrators.

However, since December 2023, we have seen a significant increase in anonymous bomb threats. Threats have started to appear more and more frequently, and large groups of subjects have been targeted at the same time. This trend has led to increased fear in society, overstretched security forces, and significant time and financial losses in the affected organizations.

In the third quarter of 2024, there was an increase in attackers' interest in publicising and publishing information about bomb threats in the media, a significant shift compared to the second quarter of the same year. A local television station in eastern Slovakia even published a complete screenshot of the threatening email, including links to the attacker's profile and communications via Telegram, which triggered an increase in traffic and popularity of the aforementioned Telegram account.

While in the first half of 2024 the main targets were educational institutions, in the third quarter the range of targets has broadened considerably. Bomb threats have also begun to target airports, nuclear power plants, municipal buildings, religious facilities, and places with high concentrations of people. This shift indicates a change in tactics by attackers, who have begun to target a wider range of critical infrastructure to increase chaos and disrupt multiple sectors.

One of the other important trends in the third quarter of 2024 is the adaptation of attackers. While in the past, reporting bomb threats was often done via conventional email services, attackers have started to make greater use of anonymisation tools such as VPNs and Mail2Tor. This transition makes it more difficult to identify the sources of threats and increases the time it requires to detect perpetrators. The anonymisation of communications poses a serious problem for investigations, as security forces have to deal with the increasing technical sophistication of attackers. This increases the need to invest in new technologies to monitor and analyse encrypted communications, and cooperation with foreign partners who have more advanced tools and experience in dealing with similar threats becomes crucial.

1.3 THREAT ACTORS

1.3.1 APT groups

In the period 2024, there have been compromising efforts primarily by Russian and Chinese groups, mainly for data theft and cyber espionage. They used various vulnerabilities, malware proliferation and social engineering methods (especially phishing and spearphishing) to do so. Increased use of AI models to streamline the activities of APT groups was also identified.

Increased activity by North Korean and Iranian APT groups has been noted during the US presidential election period, including identified attempts to compromise facilities connected to the electoral process. North Korean groups have increasingly launched campaigns in which they pose as companies offering lucrative employment opportunities to individuals in areas of interest.

In the European space, hybrid activities against Romania during the presidential elections were among the biggest events of 2024, with massive cyber-attacks accompanied by influence campaigns on social media. Given the scale of these activities, it can be assumed that this was a state-sponsored group. The Chinese APT group's penetration of US state systems and critical infrastructure was also a major compromise.

In Slovakia, we have seen attempts to compromise state institutions mainly by Russian and Chinese APT groups. Most of the identified activities were not targeted exclusively at Slovak state institutions, but Slovakia was a mass target as part of campaigns specifically directed at European Union countries.

1. 3. 2 Hactivist groups

Primarily, Russian hactivist groups have carried out DDoS attacks against state institutions, NGOs, and private companies, mainly in the European space and NATO countries, for ideological reasons. The main reason for the attacks was that the targeted countries provided financial, military, or humanitarian support to Ukraine. The attacks were also carried out in the context of the European Parliament elections. Russian hactivist groups also began to launch attacks on Taiwan on a larger scale towards the end of the year. Among the most prominent groups were Killnet, NoName057(16), Cyber Army of Russia Reborn, HackNeT and the DDOSIA project.

One of the most notable activities of hactivist groups in 2024 was the penetration of systems that controlled water infrastructure in the US by the Cyber Army of Russia Reborn group. The group is believed to be affiliated with the Russian APT group Sandworm. This APT group is known for masking its activities through various hactivist groups.

In Slovakia, hactivist groups carried out attacks against Slovak targets at a much lower rate than in 2023. Increased activity was identified in the first half of 2024, but even this represented a much smaller number of attacks than in 2023. A series of attacks occurred after an attempted assassination of the Prime Minister of the Slovak Republic. For the rest of the year, attacks by hactivist groups in Slovakia were carried out sporadically.

1. 3. 3 Criminal groups

Criminal groups have carried out ransomware attacks against private companies, hospitals, service providers and the government. The groups carried out their activities opportunistically, with the aim of maximising profit. Most notable were the activities of Qilin, Medusa, INC Ransom, LockBit, BianLian, RansomHub, and Lynx Ransomware.

In the Slovak Republic, the activities of the criminal groups LockBit, RANSOMHUB, MI-MIC, MEDUSALOCKER and YZQE have been identified in a number of incidents.

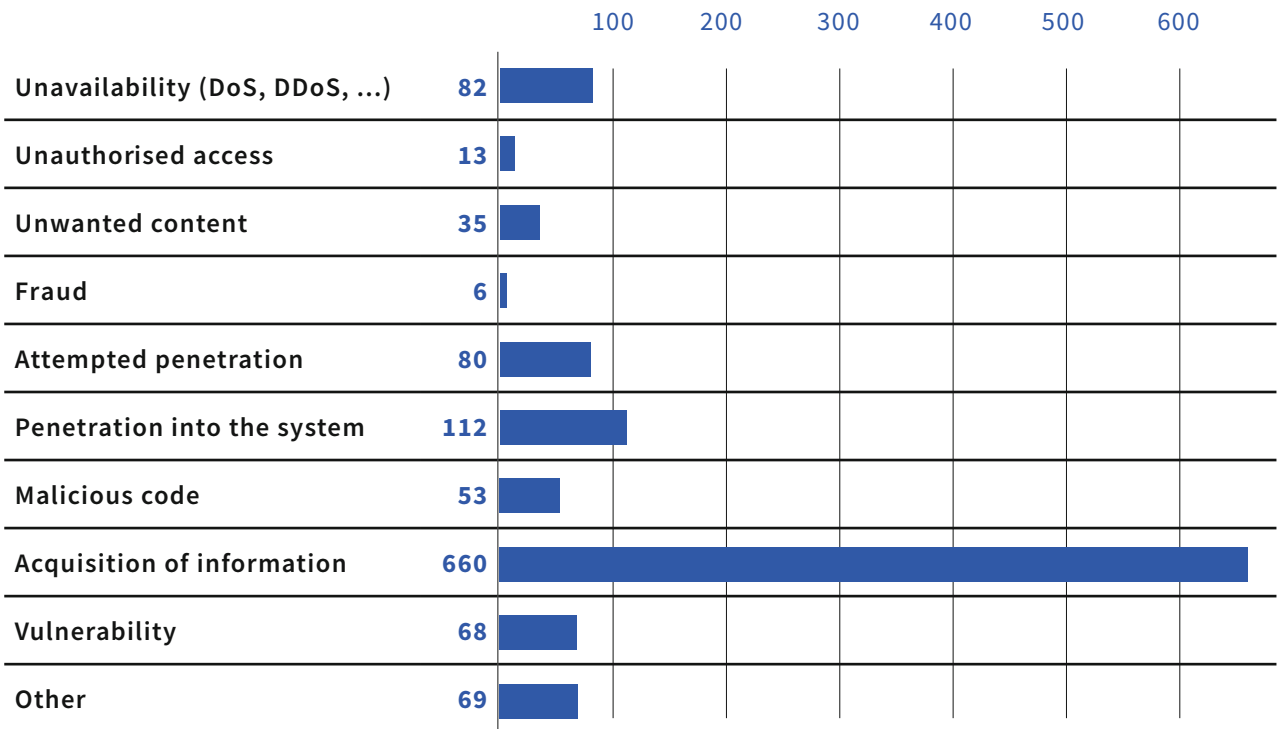
2 STATISTICAL OVERVIEW OF INCIDENTS

2.1 BASIC OVERVIEW

The National Cyber Security Centre (NCSC) performed tasks in the area of monitoring Slovak cyberspace. It worked on collecting and analysing information from received reports of cybersecurity incidents.

The statistical evaluation of cybersecurity incidents is based on the methodology introduced in 2023 and includes only incidents reported to NCSC.

TYPE OF INCIDENT REPORTED



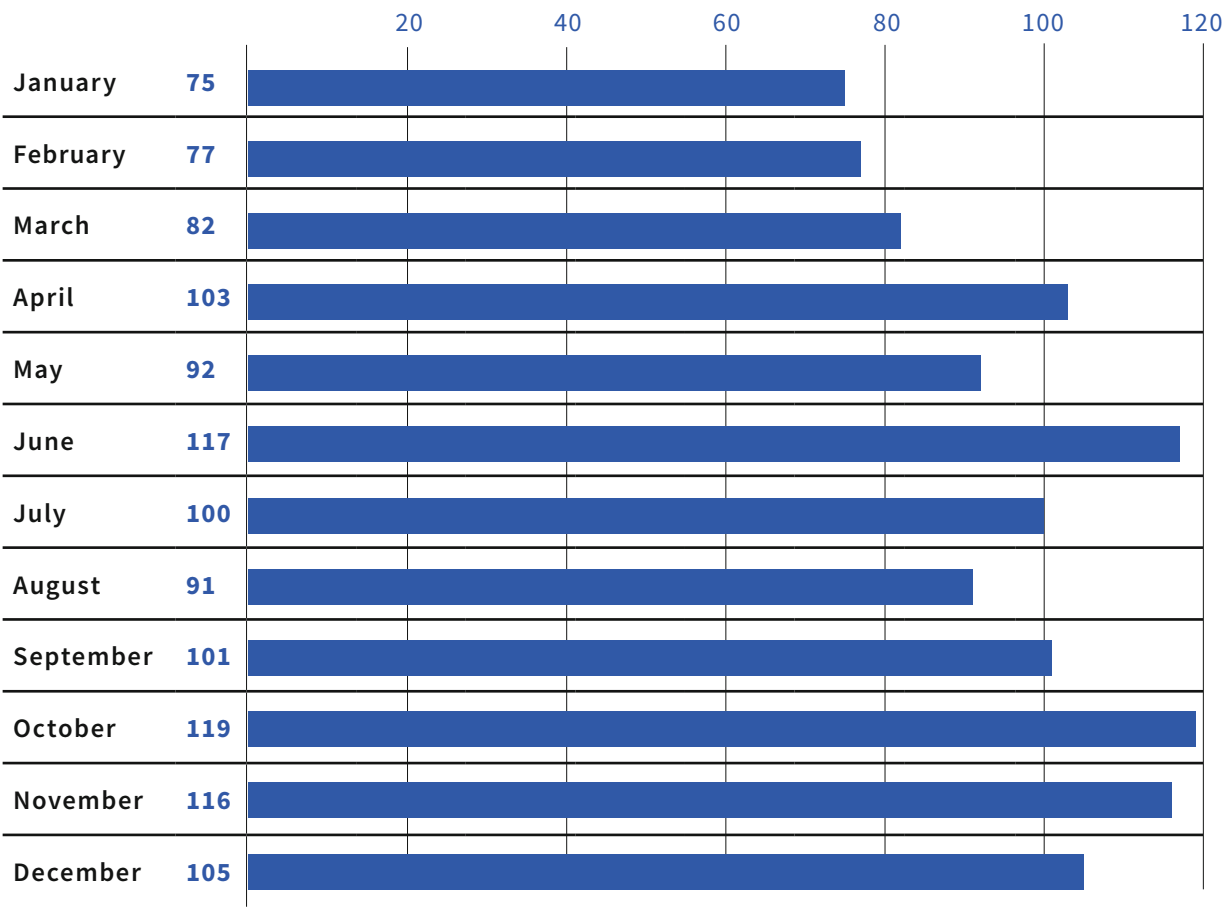
In 2024, technical attack types such as information extraction, unavailability, penetration, attempted penetration and vulnerability dominated.

Phishing has consistently been the most widespread and successful method of obtaining sensitive data and spreading malicious content. Unavailability includes the unavailability of systems that is not the result of a cyber-attack (see above). Compared to the previous year, we have seen an increase in ransomware and malware activity.

In 2024, most reports of cybersecurity incidents were received in the second half of the year. In 2024, SK-CERT received 204 more reports than in the previous year. The increase in reported incidents can be attributed to the legislative process of transposing the NIS2 directive, which extends its scope to additional entities. The public discussion on the amendment to the Act No. 69/2018 Coll on Cybersecurity (Cybersecurity Act) has undoubtedly raised awareness regarding the obligation to report incidents. Therefore, the increased number of reported incidents does not allow us to draw a clear conclusion that Slovak cyberspace has become less secure.

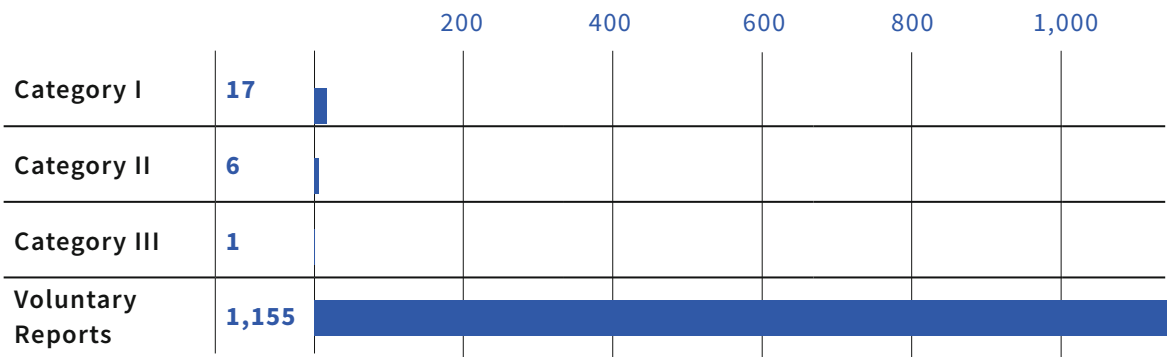
The overall numbers of reported incidents in the opposite direction are influenced by the continued ignorance or reluctance to report incidents among some Operators of Essentials Services (OES) and Digital Service Providers (DSP), but also by the increasing sophistication of malicious activities of threat actors, which are more difficult to detect.

NUMBER OF REPORTED CYBERSECURITY INCIDENTS OVER TIME



Voluntary reporting significantly outnumbered mandatory categorised reporting. Differences in maturity and legal awareness of OES persist, resulting in non-reporting, delayed reporting or a preference for voluntary reporting over mandatory reporting of serious incidents.

INCIDENT REPORTS BY SEVERITY



2.2 INCIDENTS BY SECTOR

In 2024, the number of reported cyber incidents increased. However, this trend is not reflected in all sectors.

In the banking sector, we are seeing a reduction in the number of security incident reports. This sector continuously reports the best results from audit reports and cybersecurity assessments.

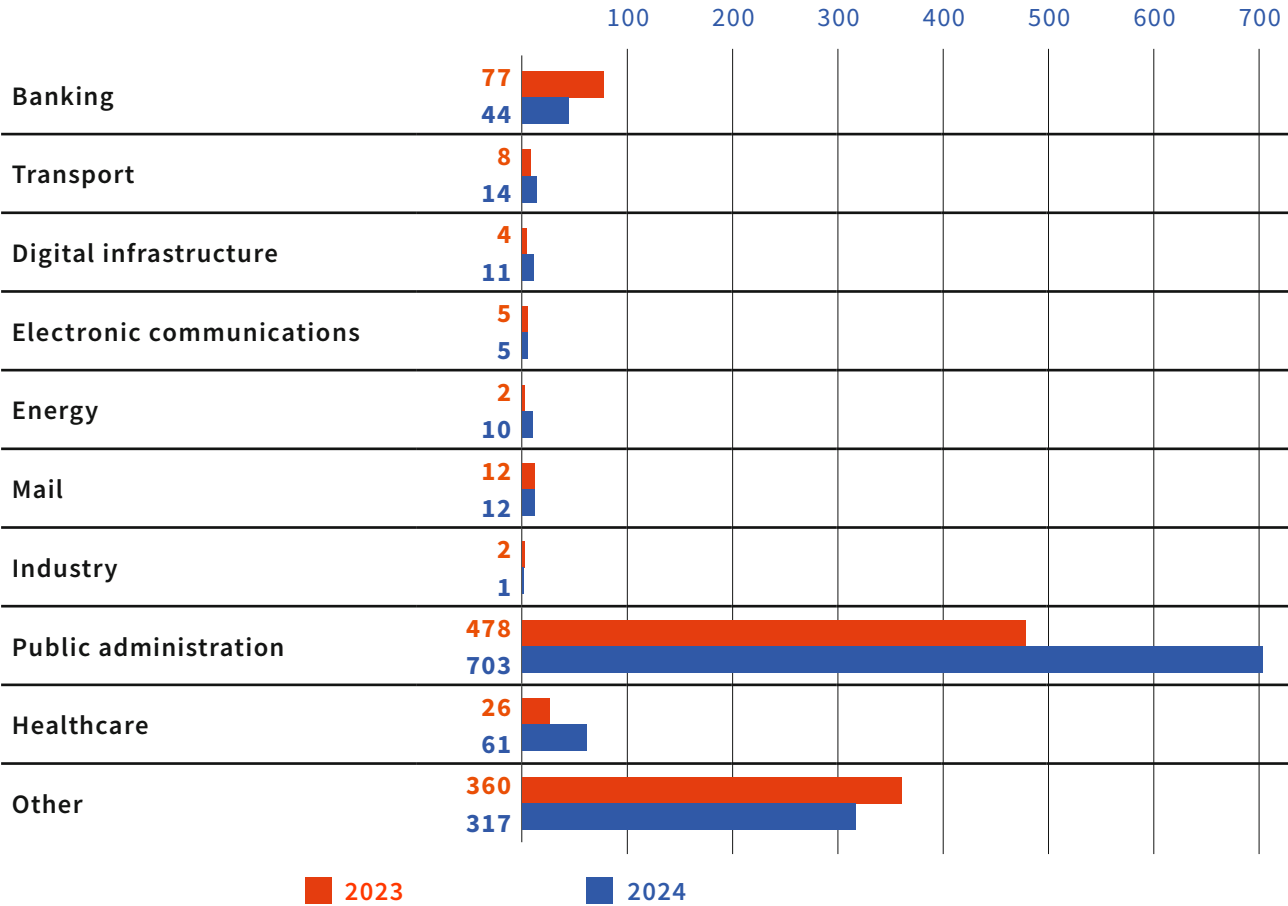
Most incidents were reported in the public administration, where the number of incidents increased significantly from 478 in 2023 to 703 in 2024. This increase may indicate both an increased threat, i.e. the motivation of attackers, but also an improvement in the detection and reporting of incidents.

The healthcare sector saw a significant increase from 26 to 61 incidents, reflecting the increasing interest of attackers in sensitive data and the often weaker technical preparedness of healthcare facilities.

Energy and digital infrastructure have also seen a rise in reported incidents, which may be a response to rising geopolitical tensions and increasing reliance on digital technologies.

Post, electronic communications and transport remain stable or have seen a slight increase.

The table reveals important trends and highlights the need to further strengthen cybersecurity, especially in key sectors such as public administration, healthcare and energy.



3 THE STATE OF CYBERSECURITY

3.1 OVERALL VIEW

To assess the state of cybersecurity in the Slovak Republic in 2024, the audit reports of individual OES, which were delivered to the National Security Authority (NSA) as well as the outputs of some central authorities, were analysed.

The overall state of cybersecurity was improving across sectors in 2024. However, there are still significant differences between sectors in their approach to cybersecurity, as well as in the level of compliance with relevant obligations and application of security measures. These differences can be observed in staffing, processes and also at the technological level. While the level of cybersecurity in the banking and electronic communications sector is high, the public administration, healthcare and water and atmosphere sectors still lag far behind.

In the public administration sector, partial improvements are being made at the level of some OES, especially in the ability to identify and assess vulnerabilities (mainly thanks to the Achilles project operated by the Ministry of Investment, Regional Development and Informatisation of the Slovak Republic) and to detect cybersecurity incidents. However, there is still a lack of a conceptual approach in the management of cybersecurity and the systematic application of security measures in their interconnection and link to real risks. There also appears to be a lack of effective addressing and remediation of already identified vulnerabilities. Some critical vulnerabilities are tolerated for a considerable length of time, while the risk of their exploitation by attackers increases significantly over time. Overall, this state of affairs is caused not only by the lack of cybersecurity strategies and policies in ministries and entities, the absence of systematic risk management or a clear division of responsibilities, but also by the lack of cybersecurity specialists and the system of funding for IT and cybersecurity in the public administration. Funding is generally inadequate (investment debt), inefficient and unbalanced in terms of resources (own/EU, operational/capital), in particular the phenomenon of the use of EU funding through various project calls, which is ad hoc and often does not take into account the needs, risks or shortfalls of cybersecurity actors. This is particularly the case when project funding is not adequately complemented by own financial resources for other needs outside the scope of the project calls, such as human resources and operations.

Another sector in which it is essential to increase efforts and support in the area of cybersecurity is healthcare. In this sector, there are still very large differences between operators in terms of their level of cybersecurity. In particular, the largest state-owned healthcare providers are constantly struggling with underfunding problems, which are manifested in a lack of resources in the areas of IT and digitalisation as well as in the area of cybersecurity.

3.2 AUDITS AND SELF-ASSESSMENTS

The cybersecurity audit verifies the fulfilment of obligations under the Cybersecurity Act, assessing the compliance of the adopted security measures with the requirements under this Act and the special regulations that apply to the security of the networks and information systems of the OES for the individual networks and information systems of the service and for the means that support the services. The objective of the cybersecurity audit is to measure, ensure the required level of cybersecurity, prevent cybersecurity incidents and identify deficiencies in the provision of cybersecurity by the OES. It also aims to propose and take measures to address these deficiencies and rectify the existing situation.

In 2024, 202 audit reports were received by the NSA.

Self-assessment, i.e. verification of the effectiveness of the adopted security measures and the fulfilment of the statutory requirements by the cybersecurity manager, OES, was not carried out by the NSA in 2024. It was possible to carry out a self-assessment until 31 December 2023.

As for the actual assessment of the state of cybersecurity from audit reports, it should also be noted that this approach has limitations. One of them is the two-year cycle of mandatory audits. This means that in a given calendar year, only a proportion of entities will deliver audit reports, which is quite low in some sectors. The approach is inconsistent and often results in unsystematically structured content, which cannot be easily compared or processed into aggregated outputs.

2024 is the year in which relatively few OES are required to be audited under Section 29 of the Cybersecurity Act on a two-year cycle. For this reason, the low number of audits in certain sectors is not a suitable basis for a more detailed assessment of the state of cybersecurity in the given sector. For example, in the industry sector, the NSA received only one audit report. An assessment of the state of security in sectors where only one or no audits were conducted was not possible and is therefore not part of this report. Only in the public administration sector was a higher number of audit reports submitted (163), and therefore, only in this sector does a more detailed view of audit findings hold significance.

In the future, it will be necessary to develop other ways of systematically collecting data from sectors and from individual actors in such a way that they can be more easily analysed in terms of their meaningful value (quantitative and qualitative indicators), aggregated and visualised. The benefit should be not only a more comprehensive and objective view of the state of cybersecurity and the dynamics of development, but also a meaningful measure for individual sectors and OES.

3.3 STATE SUPERVISION

In 2024, the NSA carried out inspections at a total of 16 OES. Deficiencies were found in 14 of these operators. In 2024, the inspection teams recorded a total of 117 findings in the following areas:

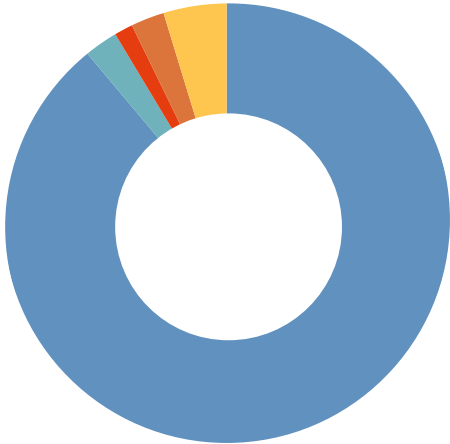
- › cybersecurity and information security management in relation to third parties - **10 violations**
- › event logging and monitoring of networks and information systems with - **8 violations**
- › risk management - **19 violations**
- › asset management - **3 violations**
- › identification of technical vulnerabilities - **4 violations**
- › cyber security incident response - **17 violations**
- › classification of information and categorisation of networks and information systems - **3 violations**
- › content and structure of security documentation - **6 violations**
- › managing the security of network and information systems operations - **11 violations**
- › personnel security - **2 violations**
- › network and communications security - **6 violations**
- › control of access of persons to the network and information system - **10 violations**
- › cybersecurity Manager Designation - **2 violations**
- › concluding a contract to ensure compliance with security measures and notification obligations under the Act - **4 violations**
- › failure to deliver a cybersecurity audit - **3 violations**
- › no cybersecurity strategy - **2 violations**

3.4 BANKING SECTOR

The NSA received a total of five audit reports from the banking sector as of 31 December 2024. Based on audit compliance statistics, the average compliance percentage in the banking sector is as follows:

BANKING SECTOR ASSESSMENT

COMPLIANCES	89,05 %
PARTIAL COMPLIANCES	2,46 %
DISCREPANCIES	1,42 %
NOT APPLICABLE	2,53 %
VERIFIED ELSEWHERE	4,47 %

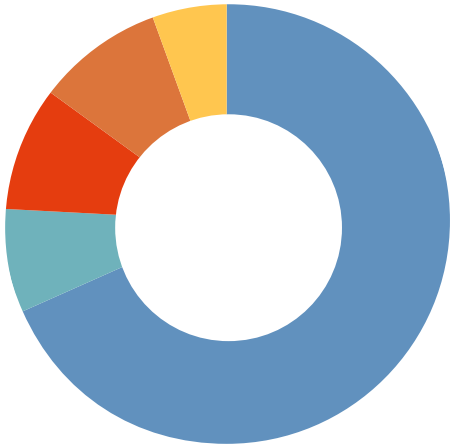


3.5 DIGITAL INFRASTRUCTURE SECTOR

As of 31 December 2024, the NSA had received a total of four audit reports from the digital infrastructure sector. Based on the audit compliance statistics, the average percentage compliance rate in the Digital Infrastructure sector is as follows:

EVALUATION OF THE DIGITAL INFRASTRUCTURE SECTOR

COMPLIANCES	64,46 %
PARTIAL COMPLIANCES	7,07 %
DISCREPANCIES	8,52 %
NOT APPLICABLE	8,88 %
VERIFIED ELSEWHERE	5,17 %

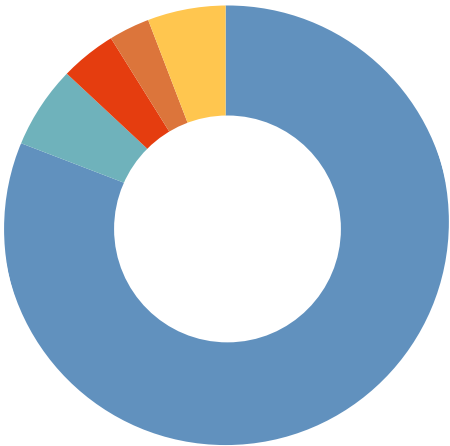


3. 6 ELECTRONIC COMMUNICATIONS SECTOR

As of 31 December 2024, the NSA has received a total of three audit reports from the electronic communications sector. Based on the audit compliance statistics, the average percentage compliance rate in the electronic communications sector is as follows:

EVALUATION OF THE ELECTRONIC COMMUNICATIONS SECTOR

COMPLIANCES	81,10 %
PARTIAL COMPLIANCES	6,07 %
DISCREPANCIES	4,05 %
NOT APPLICABLE	3,15 %
VERIFIED ELSEWHERE	5,62 %

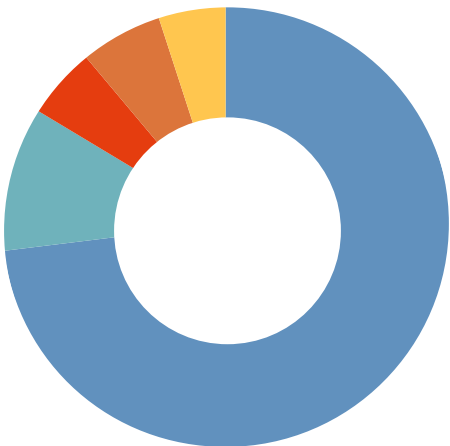


3. 7 ENERGY SECTOR

The NSA has received a total of seven audit reports from the energy sector as of 31 December 2024. Based on the audit compliance statistics, the average percentage compliance rate in the energy sector is as follows:

EVALUATION OF THE ENERGY SECTOR

COMPLIANCES	73,13 %
PARTIAL COMPLIANCES	10,49 %
DISCREPANCIES	5,41 %
NOT APPLICABLE	6,18 %
VERIFIED ELSEWHERE	4,79 %

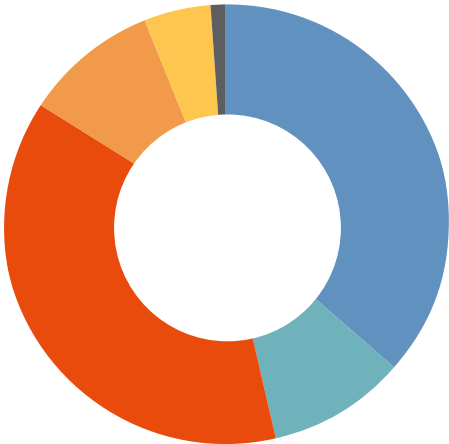


3. 8 PUBLIC ADMINISTRATION SECTOR

As of 31 December 2024, the NSA had received a total of 163 audit reports from the public administration sector. Based on the audit compliance statistics, the average compliance percentage in the public administration sector is as follows:

PUBLIC ADMINISTRATION SECTOR ASSESSMENT

COMPLIANCES	37 %
PARTIAL COMPLIANCES	10 %
DISCREPANCIES	38 %
NOT APPLICABLE	10 %
VERIFIED ELSEWHERE	5 %
UNRATED	1 %



Analysis of 2024 audit reports in the public sector has shown that key weaknesses in cybersecurity management are recurring across a number of OES. In particular, these deficiencies are:

- cybersecurity strategy defining cybersecurity objectives is not developed or is not up-to-date
- rules and procedures for information classification and information system (IS) categorisation are not put into practice
- risk and impact analysis is not carried out on a regular basis, measures put in place are not linked to the results of the risk analysis
- supply chain management is not comprehensively implemented; the OES do not have contract amendments in place to reflect the obligations set out in the Cybersecurity Act
- access and rights management policy is not defined and implemented or is not comprehensively implemented
- rules, procedures and responsibilities for IS and network security management are not formalised
- procedures for the acquisition, development and maintenance of IS and networks are not in place
- vulnerability detection systems are not comprehensively in place and there are no procedures for effective remediation or mitigation
- capabilities to detect and respond to cybersecurity incidents are not sufficient
- business continuity management procedures are not sufficiently established and updated

3. 9 WATER AND ATMOSPHERE SECTOR

As of 31 December 2024, a total of three audit reports from the water and atmosphere sector have been received by the NSA. Based on the audit compliance statistics, the average compliance percentage in the water and atmosphere sector is as follows:

EVALUATION OF THE WATER AND ATMOSPHERE SECTOR

COMPLIANCES	46,20 %
PARTIAL COMPLIANCES	22,15 %
DISCREPANCIES	21,30 %
NOT APPLICABLE	4,79 %
VERIFIED ELSEWHERE	5,54 %



3. 10 HEALTH SECTOR

As of 31 December 2024, the NSA received a total of 11 audit reports from the health sector. Based on the audit compliance statistics, the average percentage compliance rate in the health sector is as follows:

HEALTH SECTOR ASSESSMENT

COMPLIANCES	45,75 %
PARTIAL COMPLIANCES	16,93 %
DISCREPANCIES	25,54 %
NOT APPLICABLE	6,05 %
VERIFIED ELSEWHERE	5,73 %



3. 11 ASSESSMENT OF THE STATE OF CYBERSECURITY BY CENTRAL AUTHORITIES

3. 11. 1 Ministry of Investment, Regional Development and Informatisation of the Slovak Republic

The Ministry of Investment, Regional Development and Informatisation of the Slovak Republic has assessed ransomware attacks as the most serious threat in the public administration sector, which can cripple the overall operation of organisations and, under certain conditions, disable their operations for a long period of time. The Government CSIRT (CSIRT-Sk) handled six ransomware incidents during 2024. Serious threats also include phishing, which is the initial attack vector in 80 to 90 percent of cases.

As part of its proactive activities, the CSIRT-Sk used the Achilles system to perform regular non-invasive scanning and verification of vulnerabilities in services and devices of IT infrastructures of state and public administration organisations that are publicly accessible from the Internet. The service also monitors the availability of the information technologies in public administration organisations' web domains listed in its database. This situation is to be improved by the amendment to the Law on Information Technology in Public Administration, which makes it mandatory for organisations in this sector to register as a subject in the Government Information System for Cyber Security of the CSIRT-Sk. This activity affects both central authorities and other OES.

At the same time, the final phase is underway to optimize the monitoring of the entities involved in the National Agency for Network and Electronic Services (NANES) SOC and to prepare for the involvement of several other entities in the public administration sector.

In the framework of the preparation of the amendment of the Cybersecurity Act, based on the NIS2 Directive, consultations with other central government authorities were carried out. Consultations took place between the NSA, the Ministry of the Interior and the Ministry of Investment and Regional Development of the Slovak Republic.

Within the public administration sector, preventive awareness-raising activities were also carried out during the past year, mainly targeting secondary schools, but also employees of local government institutions. Awareness-raising activities were focused on the topic of safe behaviour in the online space and on social media. In total, over 3 000 secondary school students and 780 employees of public administration institutions were trained.

For the public administration, a number of calls for proposals and projects were implemented in 2024, which were open to the sector to increase their cyber and information security.

The Ministry has also launched the Central Cyber Security Portal, which provides public administration entities with up-to-date methodologies, guides, document templates, as well as news in the field of cybersecurity to increase security awareness and skills. In 2024, the Ministry trained more than 100 professionals in the newly established training and education centre - Cyber Arena.

Within the framework of prevention and supervision, the Ministry carried out more frequent inspections of security measures within the meaning of Act No. 95/2019 Coll. on Information Technologies in Public Administration and on Amendments and Supplements to Certain Acts and the relevant Decree No. 179/2020 Coll. for the entities

of public administration, as well as trainings on these inspections, thereby aiming to increase compliance with the Act among entities in the sector.

CSIRT-SK has cooperated with several sectoral coordinators, such as the Ministry of Interior of the Slovak Republic and the NSA. International cooperation within the 'CSIRT network' around the world is also important, as well as organisations represented in the Trusted Introducer or First.org associations.

3. 11. 2 Ministry of the Interior of the Slovak Republic

In 2024, the Ministry of the Interior of the Slovak Republic, as the central authority for the public administration sector in the security sub-sector, recorded slightly increased activities, threats, and dangerous actions in the area of cybersecurity targeting the ministry's infrastructure and information systems compared to 2023.

In 2024, the ministry did not record any cybersecurity incidents within its infrastructure that would be classified as serious. As a central authority, it has recorded a number of potential attempts to compromise critical infrastructure within the department's network, which have been classified in terms of incident classification as DDoS attacks on the department's internet services to disrupt their availability. In total, 9 DDoS attacks were intercepted, targeting department's services, representing a decrease in DDoS attacks of more than 50 % compared to 2023. The decrease in DDoS attacks on the department is largely due to effective mitigation at the perimeter. These attacks fall into the category of minor incidents, as in most cases they do not represent a significant impact on cybersecurity.

Furthermore, the ministry recorded 1,756 suspected cyber incident reports through the (internal) single point of contact for reporting cybersecurity incidents involving ministry infrastructure or ministry personnel. These were primarily activities of social engineering methods, with phishing attacks to compromise user accounts, followed by fraudulent emails and spear-phishing attacks being prevalent in the majority. The quality of these attacks is increasing exponentially with the development and use of artificial intelligence for social engineering purposes.

In 2024, the ministry, as the OES, conducted a cybersecurity audit of 6 essential services to ensure an increased level of compliance with the requirements of Cybersecurity Acts.

As part of its activities, the ministry was also involved in addressing various unlawful acts and other undesirable activities. However, the most serious were campaigns focused on the issue of sending threatening emails to various entities within both the state and commercial structures in Slovakia. Also serious were the actions of various foreign organized groups engaged in fraudulent activities targeting the financial resources and payment services of Slovak citizens. The scope and form of these activities evolve and change depending on the intensity of use of payment platforms and tools, as well as the popularity of certain crypto-assets.

The Department of Cybercrime mainly carried out activities related to the repressive actions of the Police Force (PF) of the Slovak Republic, as the Department of Cybercrime mainly performs practical and methodological assistance to the units of the PF structures. As part of its cybersecurity-related activities, these were generally preventive efforts in the form of alerts about the occurrence of various fraudulent activities related to the use of information technologies.

If necessary, in specific or particularly serious cases, the department cooperates with all parts of the state, but also commercial structures involved in cybersecurity or general security of the country. In cases where the nature or scale of the situation so requires, the department also cooperates with institutions operating in other European countries.

The report does not include statistics on individual types of cybercrime or computer crime due to the ongoing change in the reporting methodology for this data.

3. 11. 3 Ministry of Defence of the Slovak Republic

Military Intelligence (MI) was involved in 237 cybersecurity incidents of varying levels of severity during 2024. MI assessed the most serious activities to be those of advanced foreign state-sponsored actors, so-called APT groups, with potential impact on the Slovak Republic's defence.

There has been an increased interest of APT groups associated with the Russian Federation in critical infrastructure in the energy and transport sectors of the Slovak Republic. The subject of interest of these groups were mainly entities operating in the field of railway transport and energy raw materials transmission. In that year, the MI also analysed a phishing campaign directly directed against members of the Ministry of Defence. The tools used by the attackers in the phishing campaign were attributed to an APT group publicly associated with the Government of Iran. Other APT groups, attributed by the expert community to the Government of the People's Republic of China, focused their attention on public and private sector platforms.

Military Intelligence carried out consultations and activities aimed at identifying vulnerabilities in the information and communication infrastructure of organizations within the Ministry of Defence. On the basis of individual requests, it carried out penetration testing of several systems of the Ministry of Defence components and regular scanning of the information and communication infrastructure of several organisations belonging to the Ministry of Defence, as well as other central government bodies. In particular, it was actively involved in raising the security awareness and professional qualifications of officers and employees of the Ministry of Defence and central government and repeatedly conducted training in the field of cyber defence and security.

A special form of international cooperation for the public administration consists of cyber defence exercises. The public administration participated in several cyber defence and cybersecurity exercises organized under the auspices of the NATO Communications and Information Agency, NATO CCDCOE, and the EDA, including CROSSED SWORDS 2024, CYBER COALITION 2024, EDA milCERT Exercise 2024, NATO Crisis Management Exercise 2024, as well as national command and staff exercises focused on testing the state's cyber defence capabilities. Among the most significant was Locked Shields 2024, where Slovakia achieved 4th place overall out of 24 participating teams from approximately 30 NATO and EU countries. The joint team, composed of representatives from Slovakia and Hungary, reaffirmed its readiness and demonstrated Slovakia's key cyber defence capabilities with this placement.

4 ACTIVITIES AND ACTIONS OF THE NSA

The NSA reaffirmed its commitment to building a security environment aligned with the principles set out in the EU Security Union Strategy for 2020–2025 and the EU Cybersecurity Strategy for the Digital Decade. The priorities continue to be strengthening the resilience of cyber infrastructure, enhancing cybersecurity, and establishing processes to ensure security in both the physical and digital environments. NSA personnel contributed to the development of international relations through permanent representation in the EU and NATO, as well as by expanding additional international activities, bilateral relations, and regional cooperation.

4.1 NATIONAL LEGISLATION

The NSA systematically collects, analyses, and evaluates information from the activities of its internal departments, feedback from the expert community, requests for expert opinions, and other inputs from public authorities, legal entities, and individuals. In the field of international law, the NSA harmonizes national legislation with internationally recognized sources of law.

To transpose Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union—amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)—into the legal system of the Slovak Republic, the Authority prepared a draft amendment to Act No. 69/2018 Coll. on Cybersecurity, including amendments to related legislation (referred to hereinafter as the ‘draft law’).

The preparation of the draft law was preceded by a series of professional activities—workshops, conferences, working group meetings, and consultations with academia and the expert community at both national and international levels. The amendment to the law refines incident and vulnerability reporting, introduces a minimum level of security measures, strengthens supervisory activities, supports education, clarifies responsibilities, and enhances the role of cybersecurity managers.

The public was able to contribute to the preparation of the draft law by submitting suggestions and proposals during the preliminary public consultation (Preliminary Information PI/2024/82) held from 10 to 16 April 2024. The feedback received was discussed in consultations organized by the NSA to ensure optimal incorporation into the draft law.

The completed draft law was submitted for interdepartmental consultation through the Slov-Lex legal and information portal (legislative process LP/2024/264) from 30 May to 19 June 2024. During this period, stakeholders and the general public could submit comments. The legislative process continued with the evaluation and settlement of the submitted comments.

The draft law was discussed by the Legislative Council of the Government of the Slovak Republic on 24 September 2024, and after incorporating feedback, was submitted to the Government of the Slovak Republic, which approved it on 2 October 2024, by Resolution No. 567/2024 at its 52nd session. The legislative process continued with submission to the National Council of the Slovak Republic on 4 October 2024, where it was appro-

ved on 28 November 2024, with 117 out of 140 MPs voting in favour. The President of the Slovak Republic signed the law on 13 December 2024, and it was published in the Collection of Laws of the Slovak Republic on 19 December 2024, as Act No. 366/2024 Coll., entering into force on 1 January 2025.

To ensure protection, resilience, and improved security of entities providing services in key sectors of EU Member States, in addition to the NIS2 Directive, the following were also adopted: Regulation (EU) 2022/2554 on digital operational resilience for the financial sector, amending various EU regulations; and Directive (EU) 2022/2557 on the resilience of critical entities, repealing Council Directive 2008/114/EC. To align the national legal framework with EU cybersecurity law, the NSA actively participated in the implementation and transposition of these legal instruments.

4.2 EUROPEAN UNION

In the field of cybersecurity, the year 2024 was primarily marked by the completion of legislative activities in connection with the anticipated end of the legislative cycle in the European Parliament and the arrival of a new College of Commissioners of the European Commission. During the Belgian presidency, political discussions on the draft Regulation on Managed Security Services (CSA+) were concluded. This regulation formed part of the cybersecurity package introduced by the European Commission in April 2023.

Due to administrative complications and a lack of translator capacity, both CSA+ and the second proposal of the package - the Regulation on Measures to Strengthen Solidarity and Capacities in the Union for Detecting, Preparing for, and Responding to Cyber Threats and Incidents (CySoLa) - entered the corrigendum procedure. As a result, their final adoption took place in the new European Parliament and Council of the EU during the Hungarian presidency. These acts were published in the Official Journal of the EU at the beginning of 2025. The Cyber Resilience Act (CRA), which sets horizontal cybersecurity requirements for products with digital elements, also underwent the corrigendum procedure and was formally adopted in autumn 2024. It was published in the Official Journal of the EU in October 2024.

Slovakia, through representatives of the NSA, actively supported the objectives of most of these legislative proposals throughout 2024, providing numerous comments and suggestions during negotiations. These contributions were positively received and helped streamline and rationalise the discussed legal norms. The approval of these legislative acts is expected to enhance cybersecurity across the EU, strengthen consumer protection regarding digital products, facilitate EU-wide identity verification, and harmonize and simplify cybersecurity certification systems. However, Slovakia abstained from voting on CSA+, viewing it as duplicative of existing legal frameworks.

At the level of comitology committees, in accordance with adopted EU secondary legislation particularly the revised NIS2 Directive, the Cybersecurity Act (CSA), and other relevant regulations, the NSA participated in discussions on the implementation of specific measures. Following expert discussions with member states, the European Commission adopted in October 2024 the first implementing rules on cybersecurity for critical entities and networks under the NIS2 Directive. These rules define risk management measures and specify which types of incidents must be reported to national authorities as serious.

Within comitology activities, special attention was also given to the preparation of candidate cybersecurity certification schemes: EUCC (Common Criteria) and EUCS (Cloud Services). The EUCC scheme became operational in 2024, while preparation of the EUCS scheme was temporarily halted for political reasons.

The Horizontal Working Party on Cyber Issues (HWPCI) focused its non-legislative activities on other strategic elements of cyber diplomacy. This domain overlaps with the EU's Common Foreign and Security Policy (CFSP) and Common Security and Defence Policy (CSDP). Slovakia, along with other member states, concentrated on coordinating the EU positions in negotiations of the Open-ended Working Group (OEWG) at the UN on the use of ICTs, the Global Digital Compact (GDC), and the new Convention on Cybercrime.

Slovakia also participated in cyber dialogues with third partner countries, particularly the USA, UK, and Japan, and took part in exercises testing the Cyber Diplomacy Toolbox in practice. In response to ongoing cyber threats, Slovakia cooperated with other member states, EEAS (INTCEN), European Union Agency for Cybersecurity (ENISA), and CERT-EU, and contributed to the creation of new cyber sanctions lists targeting individuals. It also took part in the development of strategic documents outlining the EU's position toward advanced threat actors and the EU's cybersecurity stance in the Western Balkans.

In 2024, the NSA actively engaged in meetings of the NIS Cooperation Group and its subgroups, focusing on: Post-Quantum Cryptography, Elections, Health sector, and Aviation.

The NIS Cooperation Group, established under the NIS Directive, aims to achieve a high common level of security for network and information systems across the EU. Its mission includes promoting strategic cooperation, sharing of information, best practices, and aligning implementation processes with NIS2. Activities throughout the year focused on updating procedures and preparing manuals, guidelines, and other supporting documents.

Representatives of the National Cyber Security Centre (NCSC) participated in several EU-level working groups and initiatives focused on building a common cybersecurity framework. One of the most important activities was participation in the CyCLONE network, which brings together national representatives for managing cyber crises. These meetings involved strategic discussions on information-sharing and included the Cyber Europe 2024 exercise, simulating the escalation of a large-scale cyber incident in the energy sector. The goal was to improve procedures, internal cooperation, public relations response, and crisis management capabilities.

SK-CERT - national CSIRT unit (part of NCSC) also actively participated in international CSIRT organizations. Within the CSIRT Network, which brings together national CSIRTs from EU member states, SK-CERT exchanged operational threat and incident information. Due to the ongoing war in Ukraine, countries shared information and offered mutual assistance related to war-related cyberattacks. In 2024, SK-CERT maintained its 'Advanced' CSIRT maturity status—the highest level awarded through a peer-review process.

4.3 ORGANISATION FOR SECURITY AND COOPERATION IN EUROPE (OSCE)

The meetings of the participating states of the OSCE, in which the NSA actively participated in 2024, highlighted the importance of international cooperation in the field of cybersecurity and the sharing of information about existing and potential threats. Despite the high level of participation by OSCE member states, the meetings continued to be affected by the geopolitical situation, particularly the ongoing war between Russia and Ukraine, which also influenced discussions on largely non-sensitive topics such as information and communication technology security.

4.4 NATO

In 2024, meetings of the NATO Security Committee (SC) took place in all of its formats - covering security policies, communication and information system security (CISS), and the highest level involving directors of national security authorities of NATO member states. The committee was chaired by Galen Nace, Director of the NATO Office of Security (NOS), who engaged with security authority representatives on a range of security issues, not limited to the current geopolitical situation.

During the SC's spring session, representatives of national security authorities had the opportunity to visit the NATO Defence Innovation Accelerator for the North Atlantic (DIANA). DIANA uses its programs and a network of testing centres to connect start-ups with end-users, researchers, and systems integrators to support the development of cutting-edge dual-use technologies for the Alliance.

A major milestone in NATO's cybersecurity and cyber defence for 2024 was the Warsaw Summit in July, where two key documents were adopted, significantly contributing to NATO's deterrence and defence posture:

- ▶ NATO Guide for Strategic Response Options to Significant Malicious Cyber Activities, which will enhance NATO's integrated situational awareness, overall resilience, and support the process of collective action.
- ▶ The establishment of the NATO Integrated Cyber Defence Centre (NICC), which will bolster the Alliance's ability to protect its communication and information systems and strengthen the recognition of cyberspace as an operational domain within multidomain operations. As a result, 2025 will be dedicated to implementing political-military recommendations to ensure the NICC becomes fully operational by autumn 2026.

Another major NATO event in 2024 was the Cyber Defence Pledge Conference, held in May in The Hague. After a one-year break dedicated to updating the pledge questionnaire to better reflect the rapidly evolving cyber environment, ambassadors assessed the Alliance's progress in cybersecurity and cyber defence. For the first time since the pledge's introduction in 2016, member states were able to quantitatively measure progress through self-assessment, allowing for consistent comparison not only over time but also among allies and partners.

The Second Annual NATO Cyber Defence Conference, held in November in London, was another key event - not only for cyber defence, but also for broader coordination. It brought together stakeholders across all three levels - political, technical, and military, from both NATO structures and all 32 member states. Slovakia was represented by officials from the NSA and the Cyber Defence Centre.

4.5 REGIONAL COOPERATION

Based on the rotating presidency of member countries of the Central European Cyber Security Platform (CECSP), the Austrian Federal Chancellery chaired the platform in 2024. Representatives of the Slovak NSA actively participated in platform meetings alongside colleagues from the Visegrád Four countries (Czech Republic, Hungary, Poland and Austria).

The discussions focused on current issues resonating at the EU level throughout 2024, with partners seeking to find common ground and mutual support on these topics. As part of its presidency, Austria initiated a “major cleanup” of the founding documents: the Central European Cyber Security Platform – Declaration and the Working Program for the European Central Security Platform.

The most important topics of the meetings included:

- › The current status of the NIS 2 Directive transposition process in individual member states
- › Cybersecurity and cyber diplomacy
- › Cybersecurity certification – new approaches
- › The Cyber Resilience Act (CRA)

Among the member states, Slovakia was recognized as the most advanced in the transposition of the NIS2 Directive. Experts agreed that the approximation process requires an adaptive, coordinated, and innovative approach to achieve the broadest possible harmonization across the EU. In the area of capacity building, participants presented their national approaches and know-how on how to achieve set goals. Slovenia attended the meetings for the second time, and with the update of the platform’s status documents, it will now begin the process of becoming a full member. The founding countries raised no objections to Slovenia’s accession and formally approved its membership, affirming their commitment to deepening Central European cooperation in cybersecurity.

4.6 BILATERAL RELATIONS

Personnel actively developed bilateral relations across all working platforms and formats, whether through in-person contact during working group meetings or through ad hoc cooperation on bilateral tasks.

From the NSA’s perspective, the key event of 2024 was the visit of NATO NOS Director Galen Nace to the Slovak NSA in September 2024. During meetings with the Director and Deputy Director of the NSA, the NOS Director expressed interest in the NSA’s role in cybersecurity policy. The goal of the discussions was to strengthen cooperation between Slovakia and NATO, particularly in preventing cyber incidents and threats.

Following the signing of a memorandum of understanding in cybersecurity with the Republic of Kenya in the first half of 2024, representatives of the NSA visited Kenya again in October 2024 to deepen development cooperation. The visit clearly emphasized mutual efforts to exchange experience and knowledge in cybersecurity and cyber diplomacy. The Kenyan side expressed interest in participating in the CyberGame 2025 project, and further consultations and support from the NSA are ongoing.

In addition to these official visits and established bilateral partnerships, representatives of the Kingdom of Spain, specifically the Spanish National Cybersecurity Institute (INCIBE), expressed interest in cooperation and information exchange through a short visit and meetings in April 2024. The Spanish delegation was particularly interested in Slovakia's experience with the transposition of the NIS2 Directive, CRA, practical implementation, European certification schemes, and the functioning of national competence centres. Partners from Spain also shared their vision for future collaboration in these areas.

NSA and NCSC representatives regularly communicated and exchanged information with international partners, including those outside the EU, on topics such as: national-level cybersecurity legislation, vulnerabilities, threats, and incidents, best practices and lessons learned. They also participated in various international cybersecurity exercises and bilateral meetings organized under the Department of International Relations and Security Policies, which oversees regulation and supervision.

In 2024, the NSA established active cooperation with its French counterpart, the National Cybersecurity Agency (ANSSI). This partnership proved important not only for intensive cooperation on the European cloud certification scheme, but also for sharing analyses and threat reports relevant to France, including those related to the Olympic Games, European Parliament elections, and other potential threats and incidents.

Additionally, in cooperation with the International Atomic Energy Agency (IAEA), the Nuclear Regulatory Authority of the Slovak Republic, and US partners including the Office of International Nuclear Security (INS) and the US Department of Energy National Nuclear Security Administration (NNSA/DOE), collaboration continued on cybersecurity for nuclear facilities. This included specialized training focused on cybersecurity in the context of physical protection and supply chain relationships.

4.7 ISSUING WARNINGS AND BULLETINS

NCSC issued security warnings about vulnerabilities and threats. There were 51 summary security bulletins, and 701 security alerts issued.

Collectively, the NCSC alerted on 1,493 vulnerabilities and threats.

SAFETY BULLETINS AND WARNINGS

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
NEWSLETTERS	4	3	4	5	4	4	5	4	4	5	4	5
WARNINGS	53	46	53	58	50	67	57	55	80	69	65	48
TOTAL VULNERABILITIES	101	79	131	149	97	129	134	139	130	157	135	112

4.8 CYBERGAME

More than 2,300 participants registered in the third edition of the national CyberGame cybersecurity competition. During ten weeks they solved tasks of different focus, prepared by NCSC.

In 2024, the competition included three analytical branches - malware, forensics and OSINT analysis. Another gaming branch was dedicated to cryptography and the non-technical one was titled processes and security management. Offensive security was a new feature.

CyberGame is an attractive and unconventional way to find and inspire cybersecurity professionals. A total of 874 players, ranging from first-year high school students to experienced programmers, scored in the competition. Everyone had a chance to succeed, and awards were given to the overall winner, the best student, the top female player, and special recognition was given to the youngest participant, category experts, the best player from public administration, and a teacher.

4.9 AWARENESS RAISING FOR THE GENERAL PUBLIC

In 2024, the NSA developed information campaigns to raise awareness about cybersecurity. These campaigns focused on phishing threats as well as risks people may encounter while on vacation. The NSA also shared tips for parents on how to keep their children safe online. The Communications Department, in cooperation with other ministries, alerted the general public to fraud schemes spreading via email, SMS, and phone calls. The aim of these efforts was to raise awareness about threats and warn people about scammers' tactics. On its social media platforms, the department also addressed the topic of cyberviolence against women. In the 2023/2024 academic year, NSA personnel also taught a course titled Security and the Work of Journalists in Online Space at the

Department of Journalism at Comenius University in Bratislava. They educated future journalists on cyber hygiene, data, privacy, and communication protection, as well as working with open sources. The Authority also accepted an invitation to speak at a primary school in the village of Kriváň, where they discussed telephone and text-based scams with students. This continued a tradition of similar outreach activities from previous years.

4. 10 ACTIVITIES OF THE CSCCC

In 2024, Cyber Security Competence and Certification Centre (CSCCC), a state-subsidized organization, served as Slovakia's National Coordination Centre (NCC-SK) within the network of European coordination centres and the European Cybersecurity Competence Centre, in accordance with EU Regulation 2021/887. Its accreditation by the European Commission confirms CSCCC expertise and capacity to manage EU cybersecurity funding from directly managed EU programs.

That year, CSCCC signed a grant agreement with the European Commission for a new NCC project for 2025–2028.

As part of its activities, CSCCC launched an FSTP – Cascade Funding call under the NCC project funded by the Recovery and Resilience Facility (RRF). The goal was to significantly support entities in securing funds for their cybersecurity needs. A total of 46 entities successfully submitted projects in response to the call.

One of CSCCC key objectives in 2024 was the intensive development of a professional cybersecurity community. This effort led to the creation of strong partnerships, the sharing of best practices, and increased awareness of the importance of cybersecurity across business, academia, and the public sector. Through NCC-SK, 162 Slovak entities became members of the European cybersecurity community as defined by Regulation 2021/887.

As of 1 January 2024, with authorization from the NSA under § 59 of Act No. 215/2004 Coll. on the Protection of Classified Information, CSCCC is authorized to:

- Assess security projects of technical equipment under § 56(2) of the Act.
- Verify the compliance of technical equipment with security requirements and approve their use under §§ 2 and 5 of Decree No. 339/2004 Coll. on the Security of Technical Equipment.

Entities such as manufacturers, authorized representatives, importers, distributors, or users may request the evaluation of devices regarding the prevention of information leakage through unintended electromagnetic emissions. In 2024, more than 40 such assessments were conducted.

CSCCC also performed 47 cybersecurity audits during the year.

The number of certified professionals increased in 2024 by 14 certified auditors and 37 certified managers.

CSCCC was successful in the area of adult education as well. An updated training scheme was published, introducing new specialized courses and workshops such as Supplier Management and Business Continuity Management. Syllabi for several existing courses were also updated. A total of 53 training sessions were conducted in 2024: 8

courses on Cybersecurity Fundamentals; 20 Cybersecurity Manager courses; 3 Cybersecurity Auditor courses; 7 specialized courses and workshops; 1 course on Information Security Management under ISO/IEC 27001:2022; 10 free webinars on Cybersecurity Awareness; 1 seminar on the transposition of the NIS2 Directive; and 1 webinar on how to write a project and obtain EU funding. Altogether, these training activities reached 961 participants in 2024.

CSCCC representatives also actively participated in conferences and events in Slovakia and abroad, delivering 47 professional lectures, including at selected Slovak universities.

As part of its awareness-raising efforts, CSCCC published informational leaflets on topics such as:

- › Categories of Personal Data
- › What is Ransomware and How to Protect Yourself
- › 10 Management Mistakes That Lead to Security Incidents
- › How Strong is Your Password?
- › Most Common Password Attack Types
- › Cybersecurity 2024 – Public Opinion Survey Summary

Annual public cybersecurity surveys are conducted on behalf of CSCCC. In 2024, a survey of 1,000 respondents was conducted to assess public awareness and concerns.

CSCCC also continued to expand its network of partners by signing additional memorandums of cooperation.

In collaboration with SK-CERT, CSCCC formed a team of young cybersecurity talents who represented Slovakia at the European Cybersecurity Challenge (ECSC) in October 2024 in Turin, Italy. The ECSC is organized by ENISA and hosted 44 national teams. The Slovak team consisted of ten young talents—nine boys and one girl—who had trained for several months. Their preparation included attending an international bootcamp in Vienna in June and six training camps in Brunovce. The team is now continuing its preparation for ECSC 2025.

