NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

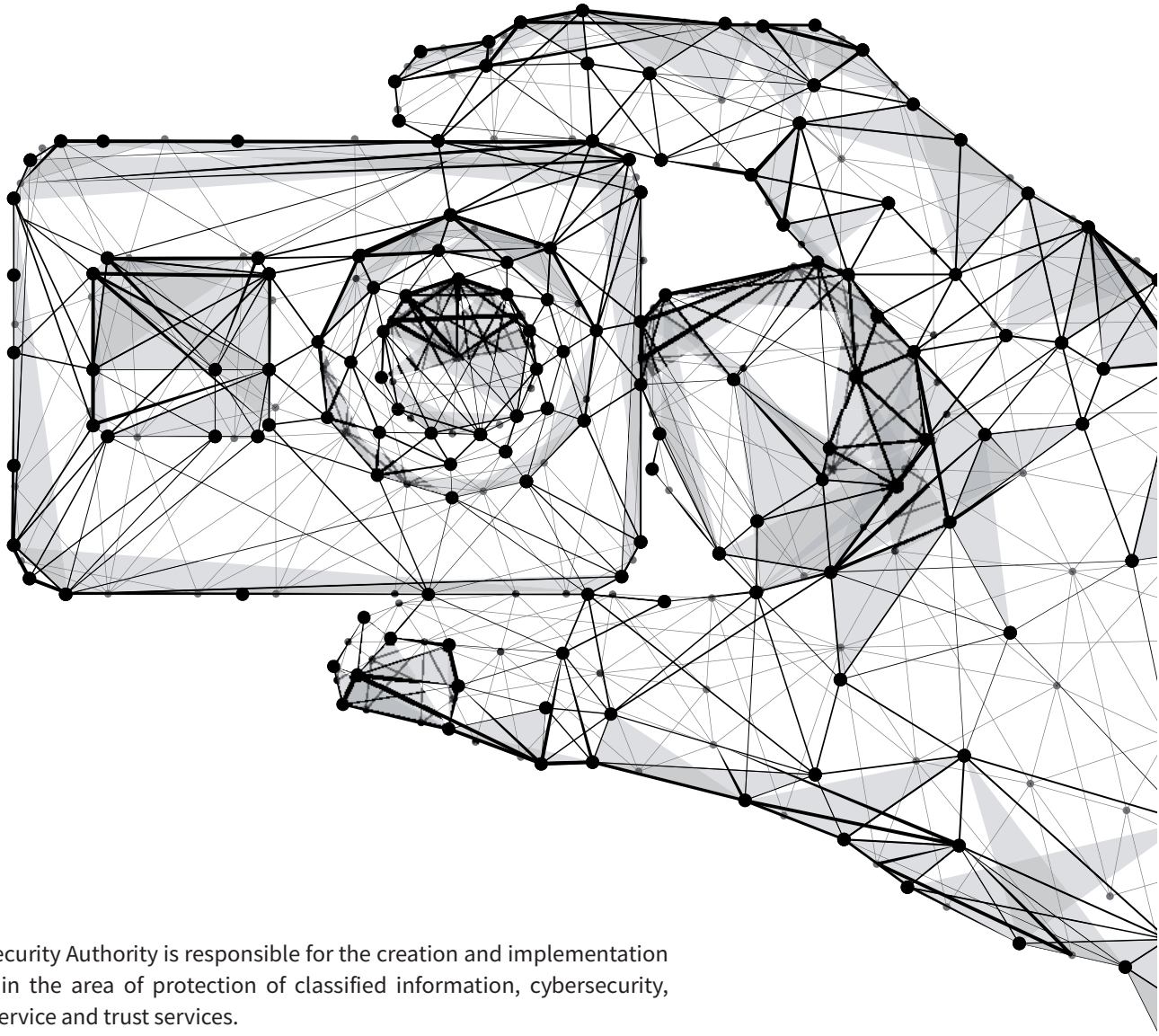
ANNUAL REPORT 2022

NATIONAL SECURITY AUTHORITY

ANNUAL REPORT 2022

CONTENTS

ORGANISATIONAL IDENTIFICATION



The National Security Authority is responsible for the creation and implementation of state policy in the area of protection of classified information, cybersecurity, cryptographic service and trust services.

In the area of protection of classified information, the NSA carries out security clearances of natural persons and entrepreneurs, comments on nominees in accordance with international agreements by which the Slovak Republic is bound, and keeps records related to the protection of classified information.

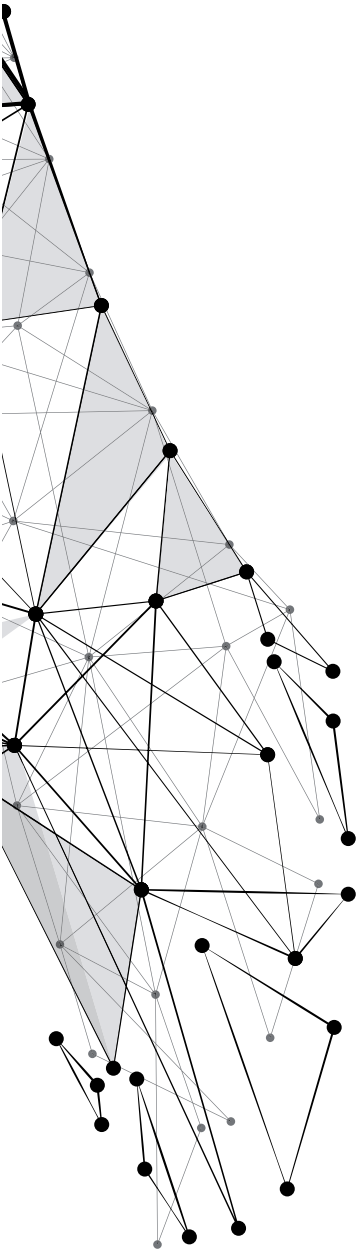
Furthermore, the NSA carries out certification of communication and information systems for handling of classified information, gives authorization to state bodies or authorization to entrepreneurs for certification of technical device and verification of conformity of mechanical barrier devices and technical protection devices with

security standards; carries out certification of technical, system, mechanical barrier and technical protection devices.

The National Security Authority performs assessment of secured areas for entrepreneurs and government bodies, including the assessment of ensuring protection of exchanged classified information and assessment of conditions for protection against undesirable electromagnetic radiation of technical devices and cryptographic protection of information devices.

The NSA provides the administration and operation of the information systems entrusted to the NSA, including the management of user accounts, ensures the administration and operation of systems of classified government and classified foreign communications, and carries out security oversight of network and application parameters of communication and information systems for the protection of classified information.

In its own capacity, the NSA conducts inspection of conditions ensuring protection of classified information in state, municipal bodies and at entrepreneurs, and publishes methodological guidelines for individual aspects of classified information security.



It further performs activities strengthening security awareness and conducts a security officer‘s examinations.

Within international exchange of classified information, the NSA performs a role of the Central Registry of the exchange of classified information in Slovak Republic and participates in the protection of foreign information.

Within the field of regulation and methodology, the NSA issues security standards, official statements and methodologies on generally binding legal regulations and documents that fall within the competence of the Authority, prepares proposals of generally binding legal regulations for the legislative process, comments and prepares official statements on proposals of legislative materials in the interdepartmental comment procedure.

The NSA provides methodological guidelines to state authorities, entrepreneurs and natural persons in all areas of its competence. The Authority also publishes anonymized methodologies and expert opinions on its website.

Within the field of cryptographic protection of information (CPI), the NSA fulfills the role of the central cryptographic body of the Slovak Republic. The NSA certifies its devices, issues security standards and coordinates research and development of information protection encryption devices. Last but not least it serves as national authority guarantor within international cooperation and provides the function of the National Distribution Authority, which is the entry and contact point of the Slovak Republic for exchange and distribution of CPI devices and cryptographic materials through the National Distribution Authority and performs the tasks of the National Distribution Authority for the distribution of NATO and EU COMSEC material.

In the field of trust services, the NSA performs the task of supervisory authority. The NSA conducts tasks related to the issuing and withdrawal of qualified status for services provided by a qualified trust service provider, which publishes in a trusted list with information on trust services.

It also conducts tasks related to the certification of devices for the production of qualified electronic signatures and qualified electronic seals; it creates, manages and

publishes a list of authorisations for the purpose of issuing mandate certificates.

It operates the Root Certification Authority in the Slovak Republic, which maintains a database of qualified certificates issued by providers supervised by the NSA and whose validity status provides indefinite information about their validity during their interval of use; enables the issuance of public key certificates to qualified trust service providers.

In the area of cybersecurity, the NSA is the national authority for cybersecurity.

It manages and coordinates carrying out of state administration in the field of cybersecurity, determines the standards and issues policy of behaviour in cyber space.

The NSA is the primary point for foreign countries in the area of cybersecurity, cooperates with central authorities, operators of essential services and digital services providers, accredits CSIRT units and cooperates with security analytical units for the purpose of exchanging and sharing information on security incidents.

KEY LEGAL REGULATIONS

When fulfilling the set tasks, the National Security Authority is governed by the Constitution of the Slovak Republic, constitutional acts, legally binding acts of the European Union, international treaties that the Slovak Republic is bound by, acts and other generally binding legal regulations, resolutions of the Government of the Slovak Republic, its statute, organisational rules and other internal legal regulations setting forth the internal processes.

In the field of protection of classified information and cryptographic protection of information, the National Security Authority is regulated by the on Protection of Classified Information (Act No. 215/2004 on Protection of Classified Information and on Amendment and Supplementing of Certain Acts as amended), related implementing regulations and applicable standards.

In the field of product certification for trust services, the National Security Authority follows the eIDAS Regulation (Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market), its implementing decisions and Act No 272/2016 on trust services for electronic transactions in the internal market.

When accomplishing tasks in the field of cybersecurity and accreditation of CSIRT units, the National Security Authority is regulated by the Cybersecurity Act No. 69/2018 and the relevant decrees issued to implement the Act.

R

NR

LEADERSHIP

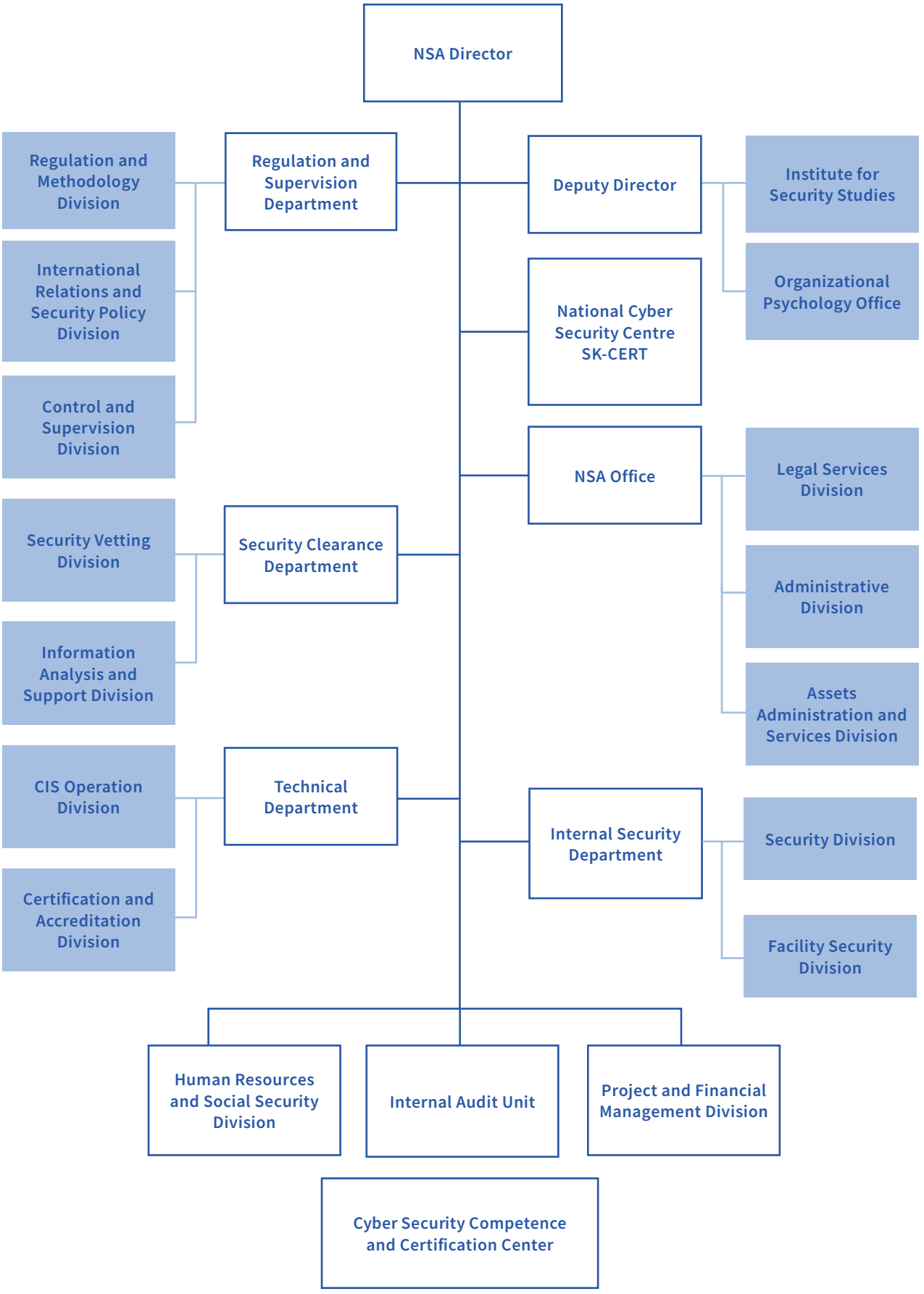
The National Security Authority is headed by the director who is responsible for its activities. Main responsibilities are to manage and represent the NSA. The director determines the implementation methodology of the main tasks of the NSA, approves the internal legal regulations, defines the internal organisational structure of the NSA and makes decisions on the personnel issues of its officers and employees.

The NSA director covers the interdepartmental cooperation of the National Security Authority and is a permanently invited member of the Security Council of the Slovak Republic.

The NSA director determines the principles of international cooperation of the NSA and in compliance with the foreign policy priorities of the Government of the Slovak Republic, supports and develops partnerships with institutions of foreign states and international organisations. In his absence, the director is in a reserved scope represented by the deputy director of the National Security Authority, who is also responsible for departmental coordination of activities.

ORGANISATIONAL STRUCTURE

The National Security Authority is organisationally divided into departments and directly managed divisions, departments are further divided into divisions.



DEPARTMENTS

NSA Office

coordinates the activities of the Authority's departments, secures and performs basic administrative and organisational activities related to the management and activities of the NSA, arranges legislative and legal matters of theNSA, builds and develops external relations and cooperation, and ensures communication to the public.

Security Clearance Department

carries out tasks in the field of personnel security and industrial security related to execution of security clearance for individuals and entrepreneurs.

Apart from security certificates and confirmations, which allow access to national classified information, it also conducts issuing of personnel security clearance certificates and facility security clearance certificates for handling of classified information of NATO and EU and expresses its opinion on individuals under international treaties by which the Slovak Republic is bound.

Regulation and Supervision Department

is responsible for the legislative tasks related to the field of classified information, cryptographic protection of information, cybersecurity, trust services and public regulated service, which is provided by the global satellite navigation system project Galileo. It fulfils tasks in areas of inspection, audit and supervision. It confers and withdraws qualified status, determines essential service and its operator, determines digital service and its provider.

It issues official statements and methodologies, creates conceptions and strategic materials, prepares security and knowledge standards, whose established procedures are introduced into international standards through ISO working groups or European standardisation institutions, issues certification and signature policies, policies of behaviour in cyberspace, principles for preventing and handling cyber security incidents. It organises and conducts security officer's examinations and training in the field of protection of classified information.

On the international level it represents the NSA and coordinates international activities of the NSA. It comments the proposals of legislative materials in the interdepartmental commnet procedure and carries out the legal process of materials with foreign elements.

Through liaison officers seconded to the Slovak Permanent Representation to the EU and to the Permanent Delegation to NATO, it performs tasks in developing and building the NSA's international relations and cooperation abroad. The liaison officers ensure communication between the NSA and foreign partners, represent the interests of the Slovak Republic in the areas of the NSA's competence in NATO, European institutions and agencies, and implement the NSA's bilateral and multilateral cooperation abroad.

National Cyber Security Centre SK-CERT

perform the tasks of the national CSIRT unit. It provides services related to the management of security incidents, their remediation and subsequent restoration of information systems in cooperation with their owners and operators, as well as analytical activities, research, security awareness and education in the field of cyber security and other tasks in the field of cyber security.

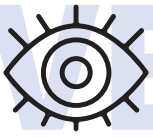
carries out duties of the national CSIRT unit. It ensures services related to handling security incidents, removing their impacts and consecutive restoration of operation of information systems in cooperation with their owners and providers. It also performs analytical tasks, research, raising security awareness and education in fields of cybersecurity and other duties in the field of cybersecurity.

Technical Department

carries out accreditation and certification activities in the field of protection of classified information for personnel, administrative security, physical security, facility security, security of technical means, industrial security, cryptographic information protection, in the field of cybersecurity, and in the field of trust services. It maintains the course and operation of information and communication systems of the NSA the management and operation of classified government and classified foreign communication systems, and also performs security oversight of the network and application parameters of communication and information systems for the protection of classified information.

Human Resources and Social Security Department

provides personnel and wage policy, social security, education and payroll. It coordinates healthcare for officers and employees of the NSA.



Internal Security Department

ensures the internal security of the NSA, performs tasks in the field of protection of classified information, ensures the physical and technical protection of the NSA's buildings, the director and the staff. In the field of internal security it obtains, concentrates, analyzes and verifies information on security risks relating to the NSA, officers and staff. It clarifies offences for departments within the NSA. It performs internal control and financial control, handles complaints and petitions. It fulfills tasks responsible entity for handling reports of antisocial activities, in the field of protection of personal data, the OPFR section on data protection and corruption prevention. It carries out tasks in the field of health and safety at work and fire protection and ensures the physical training of officers.

Project and Financial Management Department

Ensures project and program management under the terms of the office.

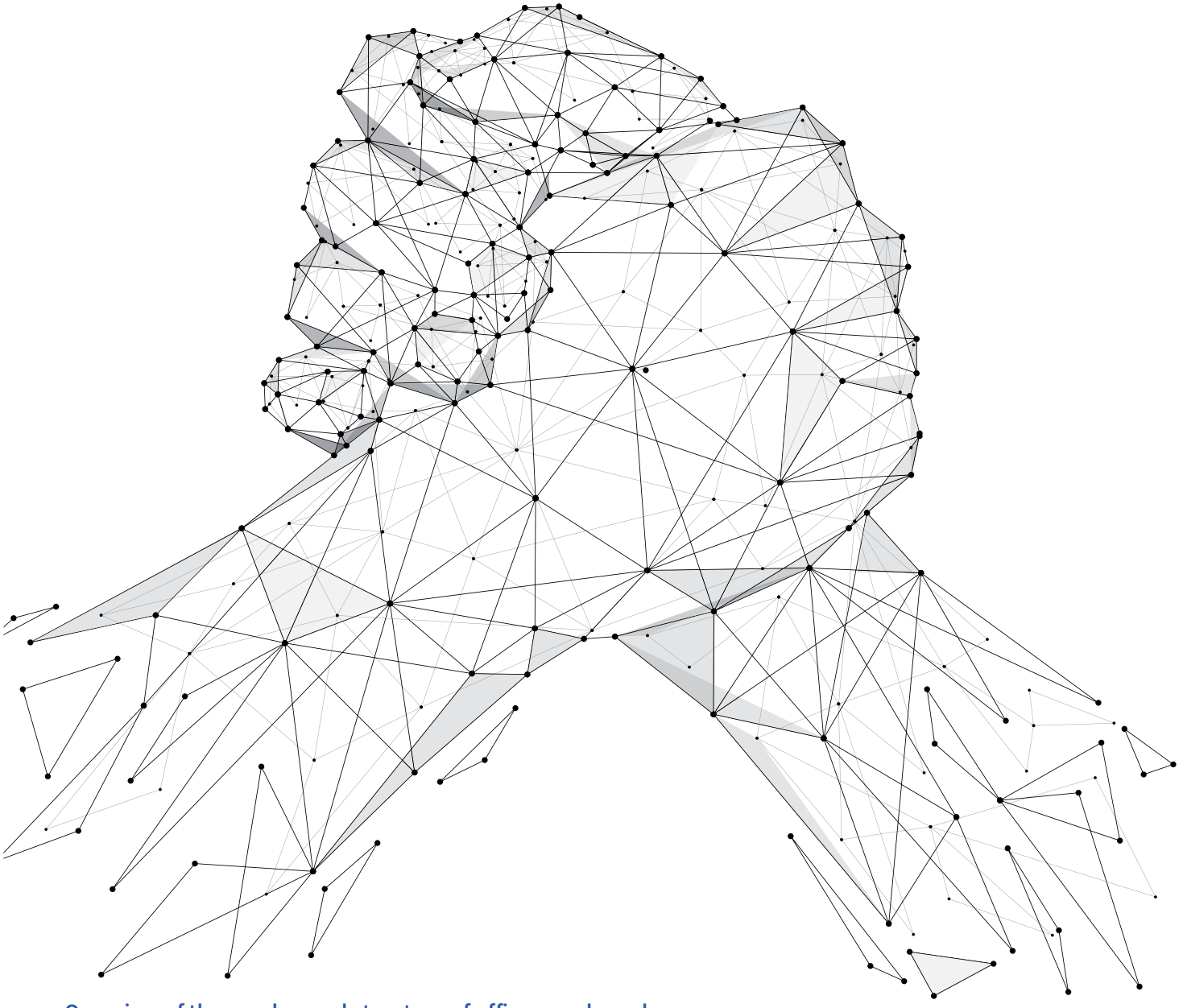
Internal Audit Unit

Ensures project and program management under the terms of the office.

Institute for Security Studies

performs tasks in the field of general analytics, security risk assessment, policy evaluation, development of forecasts, strategies and implementation plans of the NSA, as well as tasks in the field of combating hybrid threats and disinformation dissemination.

HUMAN RESOURCES



Overview of the number and structure of officers and employees

	Civil service		Employees		Officers and employees	
Preparatory civil service	**34**	16,35%				
Permanent civil service	**172**	82,69%				
Dočasná štátna služba	**2**	0,96%				
Total	**208**	90,43%	**22**	9,57%	**230**	100%

Age structure of officers and employees

	Officers		Employees		Officers and employees	
up to 34 years	40	19,23%	4	18,8%	44	19,13%
35 - 49 years old	125	60,1%	9	40,91%	134	58,26%
50 - 59 years old	39	18,75%	5	22,73%	44	19,13%
60 years and over	4	1,92%	4	18,18%	8	3,48%
Total	208	90,43%	22	9,57%	230	100%

Women and men in the NSA

	Officers		Employees		Officers and employees	
Women	107	51,44%	12	54,54%	119	51,73%
Men	101	48,56%	10	45,46%	111	48,27%
Total	208	90,43%	22	9,57%	230	100%

Educational structure of officers and employees

Officers			Employees	
0	0%	Basic education	0	0%
33	15,87%	Full secondary education	10	44,45%
7	3,37%	Higher education 1st degree	0	0%
160	76,92%	Higher education 2nd degree	11	50%
8	3,85%	Higher education 3rd degree	1	4,55%
208	90,43%	Total	22	100%

BUILDING AND DEEPENING PERSONNEL CAPABILITIES

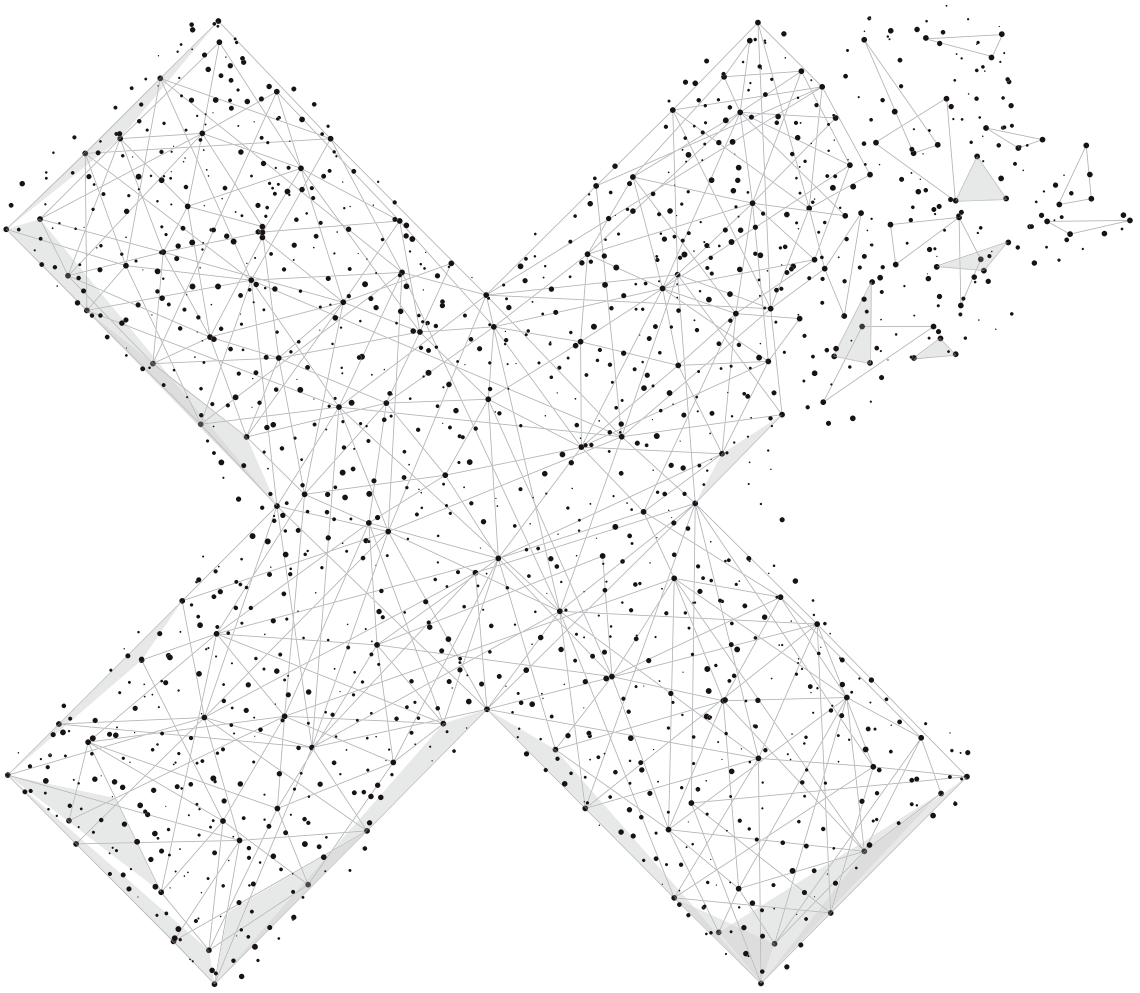
The NSA has sought to continuously streamline the training process with a view to strengthen the professional and quality staffing of the NSA, to promote the personal and professional growth and intrinsic motivation of the officers and staff of the NSA.

In the conditions of the NSA, officers and employees are enabled to maintain their professional readiness, acquire new knowledge, skills and deepen their qualifications at professional courses, seminars and training courses at home and abroad. If necessary, it enables them to upgrade their qualifications at universities.

Officers and employees receive initial training and are regularly retrained in health and safety at work, as well as fire protection.

It conducts annual specialized police training for newly recruited officers, which is a prerequisite for the placement of newly recruited officers in the permanent civil service.

Officers and employees of the NSA have suitable conditions for improving their physical fitness. In particular, members of the Internal Security Department regularly undergo shooting training, tactical exercises and simulated security scenarios in several facilities of the Ministry of the Interior and Ministry of Defense.



FIGHT AGAINST CORRUPTION

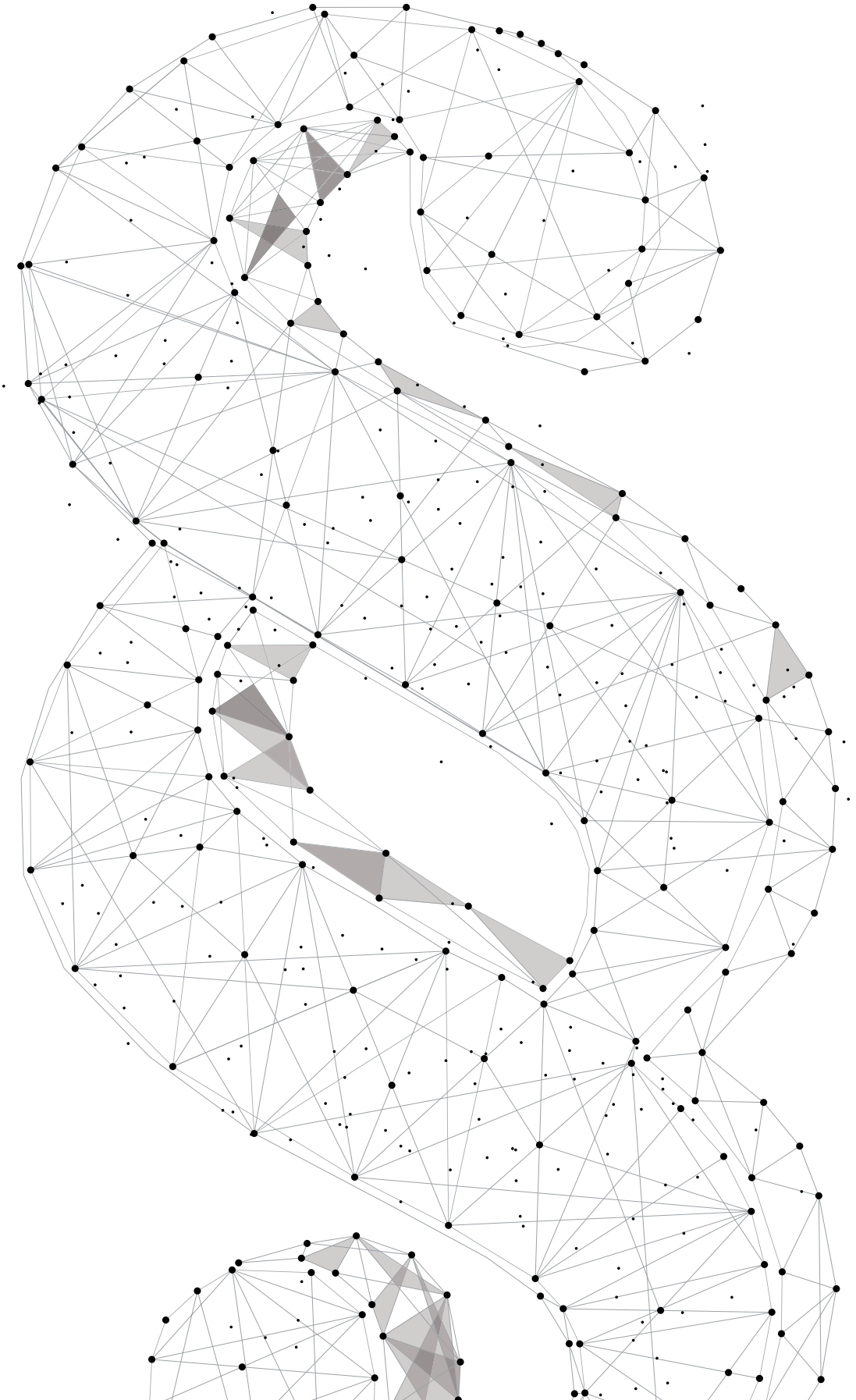
The NSA's anti-corruption programme is a tool for strengthening and promoting an anti-corruption culture and improving the management and recognition of corruption risks in the NSA's conditions.

In its anti-corruption programme, the NSA assesses and evaluates existing corruption risks and introduces specific systemic measures aimed at preventing corruption and promoting anti-corruption behavior within the NSA.

In 2022, the Authority updated the existing Anti-Corruption Programme of the NSA, which has the ambition to monitor and evaluate the setting-up of the NSA's anti-corruption system in order to address systemic failures related to corruption.

Citizens can report suspicions of corruption of officers and employees of the NSA via the anti-corruption e-mail bojprotikorupcii@nbu.gov.sk published on the NSA's website. In 2022, the National Security Authority did not receive any reports of anti-social activity in relation to its officers.

LEGISLATION



The year 2022 was fundamentally affected by the Russian military invasion to Ukraine. Conflict near the borders of Slovak Republic as a member state of the North Atlantic Treaty Organization (NATO) and new hybrid threats from the Russian Federation draw attention to the necessity ensuring and streamlining the protection of classified information.

The NSA in connection with the military conflict in Ukraine proceeded in March 2022 to **the extraordinary amendment Decree of the National Security Authority no. 336/2004 Coll. on physical security and building security as amended by Decree no. 315/2006 Coll.** This measure helped the Ministry of Defense of the Slovak Republic, which had interpretation and application problems in connection with its application in relation to protection of defense industry product, weapons, weapon systems or ammunition that is forwarded to the Slovak Republic from abroad and are classified information or contain such classified information.

The government proposed a package of extraordinary measures in Act no. 55/2022 Coll. on some measures taken in connection with the situation in Ukraine which also responded to the growing number of disinformation actors by amending Act No. 69/2018 Coll. on cybersecurity.

For the NSA was established the obligation to decide on blocking of malicious content or malicious activity directed to or from the cyberspace of the Slovak Republic and ensure even the execution of blocking with validity until 30 June 2022. Act no. 231/2022 Coll., by which amends Act no. 69/2018 Coll. was later extended this period until 3 0September 2022.

Yet in May 2022, the draft law was submitted to the interdepartmental comment procedure, by which is amended Act No. 69/2018, the purpose of which was to reflect on some questions of application practice in connection with the performance of blocking, responsibility, procedural procedure when issuing a decision and its implementation and modification of publication of decisions on the website of NSA. In November 2022, the government proposal of the Act was submitted to the National Council of the Slovak Republic (first reading).

Furthermore, the NSA implemented in 2022 the legislative process of two implementing regulations of Act no. 69/2018 Coll. on cybersecurity. The original draft of the **amendment decree of the National Security Office no. 436/2019 Coll. on cybersecurity audit and auditor's knowledge standard** in the course of the legislative transformed the process into a new proposal decree on the cybersecurity audit with the aim update the cybersecurity audit rules, its duration, periodicity and determining the appropriateness of the final report on the audit results. New decree of the National Security office no. 493/2022 on cybersecurity audit entered into force on 1 January 2023.

Decree of the National Security Authority no. 492/2022 Coll. establishing knowledge standards in the field of cybersecurity has the objective to determine the minimum professional knowledge for individual users of networks and information systems performing activities and tasks in the field of cybersecurity.

Knowledge standards also form the framework for creation educational programs at educational institutions, which fills the space not only for building high-quality security awareness in the field of cybersecurity, but also for improving quality of educational processes. This will therefore also benefit the qualification of the workers carrying out activities in the field of cybersecurity in public and private organizations.

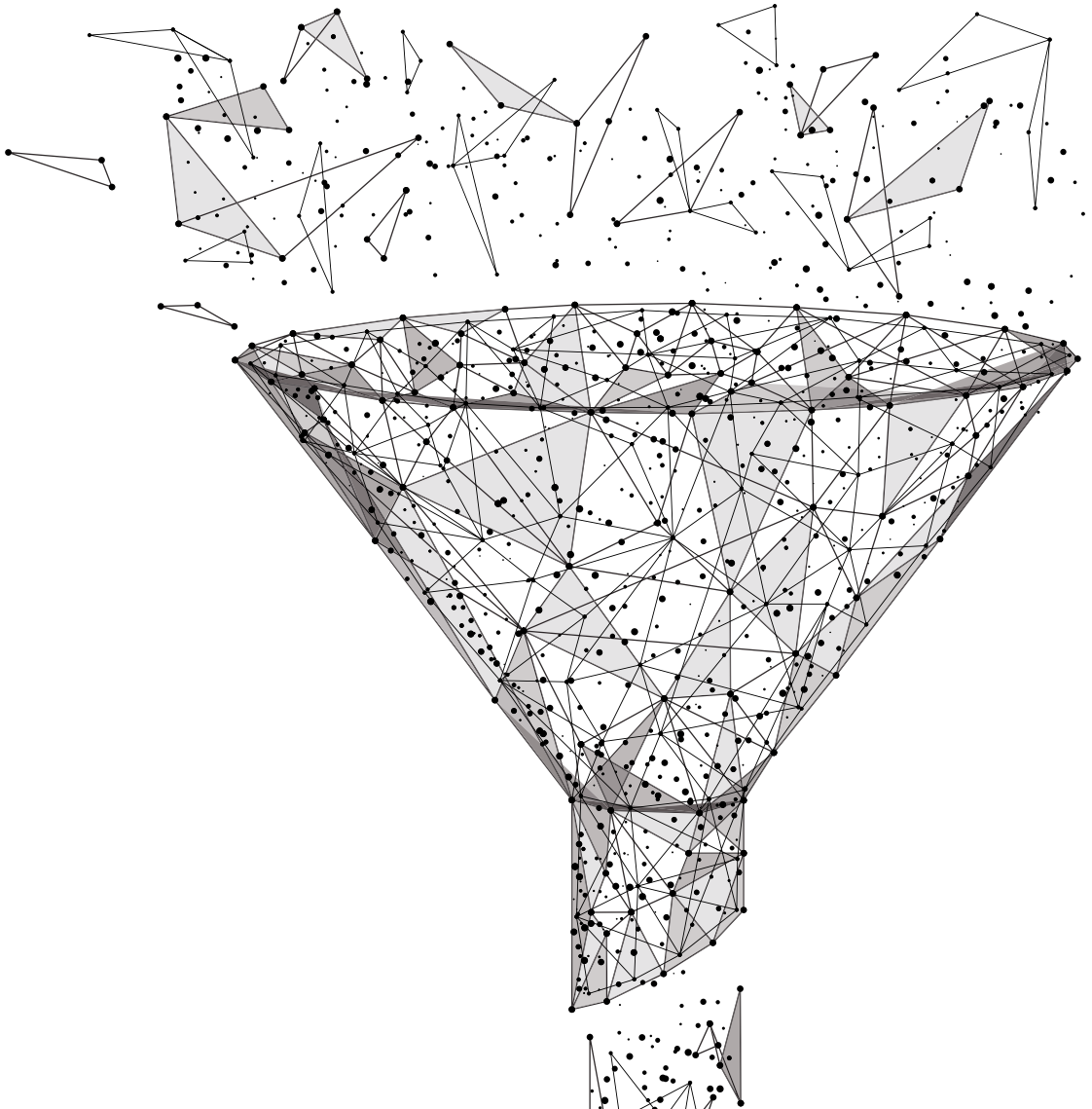
Introduction and definition of knowledge standards and their application in the field of cybersecurity is an essential element of building a stable and predictable security environment. Also this decree entered into force on 1 January 2023.

When applying **Act no. 215/2004 Coll. on the protection of classified information** in practice as the most problematic shows the fact that legislation at the level of the EU and NATO does not represent a uniform legal arrangement in the field of classified information for the member states, but applies only for protection when handling classified information, whose originator are EU and/or NATO.

The diversity of the national legislation of the member states in the field of protection of classified information in the international the cooperation of several states causes as a result application issues across all areas of security. Also in this context, the NSA had in 2022 an effort to get closer to EU and NATO legislation in the sense that when commenting on relevant legislation, the NSA wanted to relax the protection of classified information at the Restricted level, but this activity of the NSA was not understood by other public authorities, which paradoxically rather demand tightening of the protection of classified information of the classification level Restricted.

For example, the NSA tried to modify the facts in § 353 of the Criminal Code so that the facts relate only the classified information of the classification level Confidential. Thus, endangering or divulging classified information of the classification level Restricted would no longer be a criminal offence, but only a misdemeanor.

The NSA tried to specify the provisions of the criminal offenses in the Criminal Code related to the protection of classified information so that the application of these provisions in practice does not end up with purely formal deficiencies in the form of, for example, absence of the designation of classified information. The NSA had the effort to link the definitions of the facts criminal offenses in the area of classified information more closely with the definitions of the degrees of secrecy in § 3 of Act no. 215/2004 Coll., especially in relation to damage to the interests of Slovak Republic.



INTERNAL REGULATIONS

In 2022 the NSA Office issued 10 regulations of the NSA Director, 50 orders of the NSA Director, and 2 Statutes to streamline internal processes and implement generally binding legislation.

The NSA has issued a new regulation defining the responsibility of the directors of units in fulfilling the tasks of the leader arising from Act no. 215/2004 Coll. on the protection of classifieds information; regulation regulating the process of approval of the establishment of the register of classified information and the end register of classified information; regulation on executing psychophysiological verification of truthfulness; regulation on the provision of a psychological care and also amendments of regulations on domestic travel, foreign travel and the reception of foreign delegations and regulation on financial management and financial control.

New statutes were issued for the Institute for Security Studies and Organizational Psychology Office.

The orders of the NSA Director were used to identify people responsible for specific tasks – e.g. when establishing project teams, appointing members to various commissions, inventorying assets or performing of special and shooting training of officers.

ADMINISTRATIVE AND INFRINGEMENT PROCEEDINGS

In 2022, the NSA registered **17 submissions** on suspicion of committing an offense in the field of protection of classified information according to Act no. 215/2004 Coll., of which 14 submissions have been evaluated and registered as unauthorized handling of classified information. One submission was referred the competent law enforcement authority for investigation.

The NSA imposed fines for committing an offense in the area of protection of classified information in the total amount of 150 EUR and for committing an administrative offense in the area of the protection of classifieds information in the total amount of 5 600 EUR and in the area of cybersecurity in the amount of 26 000 EUR.

PROTECTION OF CLASSIFIED INFORMATION

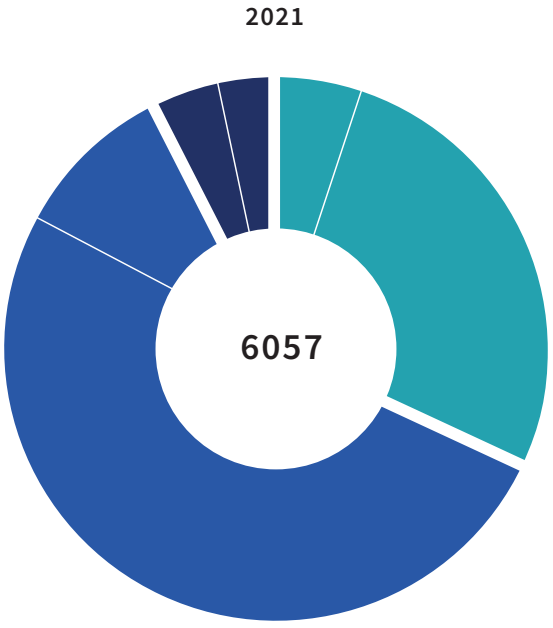
In 2022, the National Security Authority has applied all available measures to ensure that the ongoing pandemic does not affect the system of the protection of classified information

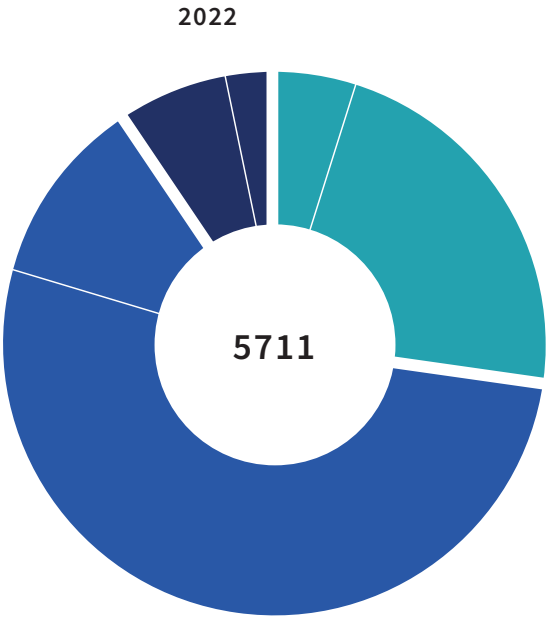
PERSONNEL SECURITY

Carrying out security checks on individuals is one of the key activities of the NSA. In 2022, the NSA issued **5711 personnel clearance certificates for acquaintance with classified information**, of which 3619 were for the Ministry of Defense of the Slovak Republic (MoD SR).

Overview of certificates issued in 2021 and 2022a 2022

Classification level	2021	2022
CONFIDENTIAL	**1947**	**1570**
of which Confidential for MoD SR	318	279
SECRET	**3662**	**3614**
of which Secret for the MoD	3034	2985
TOP SECRET	**448**	**527**
of which Top Secret for MoD SR	278	355
Total	**6057**	**5711**





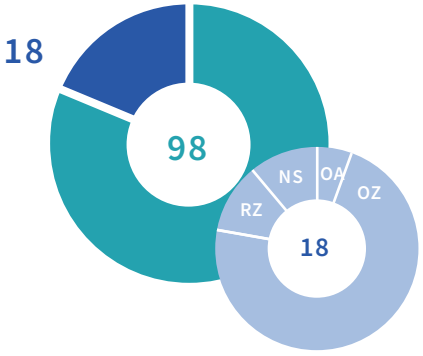
In 2022, the Authority issued 47 decisions. Natural persons filed 16 appeals against the NSA's decisions.

The NSA self-reserved the decision in two cases..

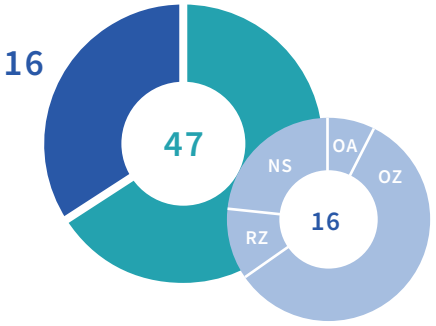
The Committee of the National Council of the Slovak Republic for the Review of Decisions of the National Security Authority decided on **18 appeals**; 15 of them dismissed and 3 decisions cancelled. As of 31 December 2022, there was one appeal pending.

Six legal actions were brought against the Committee's decision before the Supreme Court of the Slovak Republic. A summary of information on the NSA's decisions, appeals and legal actions brought before the Supreme Court is given in Table 2.

2021



2022



NSA's decisions, appeals by individuals against NSA's decisions and legal actions in 2021 and 2022

	2021	2022
DECISIONS OF THE NSA	**98**	**47**
APPEALS	**18**	**16**
Appeals – self-reversion (OA)	1	2
Appeals dismissed by the Committee (OZ)	13	15
Decisions cancelled by the Committee (RZ)	2	3
Legal actions brought before the Supreme Court (SC)	2	6

In relation to **classified information forwarded to NATO and EU** the NSA issued **7410 certificates** in 2022, of which there were issued 3703 NATO certificates and 3707 EU certificates.

Out of the total number of NATO certificates, the NSA issued 18 NATO ATOMAL certificates which authorize access to information on NATO's strategic nuclear deterrence and are issued to a narrow circle of persons.

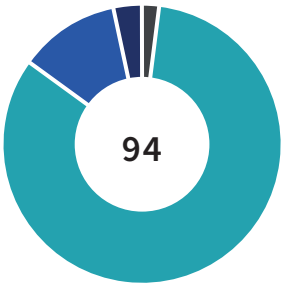
INDUSTRIAL SECURITY

In the field of industrial security, the NSA carries out **Facility Security Clearances** (FSC). An entrepreneur's FSC shall aim at obtaining information on entrepreneur who give reasonable grounds for their national authority to request the creation of classified information or to be forwarded to them.

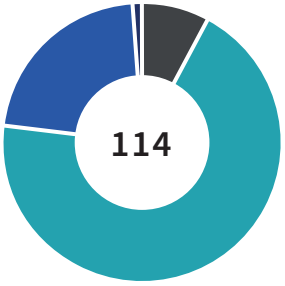
In such case, it is the duty of the statutory body of the entrepreneur to request the NSA to carry out a security clearance to obtain an **FSC certificate.**

In 2022, the NSA issued **114 FSC certificates**, 9 of them at the level RESTRICTED, 79 FSC certificates at the level CONFIDENTIAL, 25 FSC certificates at the level SECRET, and 1 FSC certificate at the level TOP SECRET. Overview of listed data is presented in table no. 3.

2021



2022



Overview of FSC certificates issued in 2021 and 2022

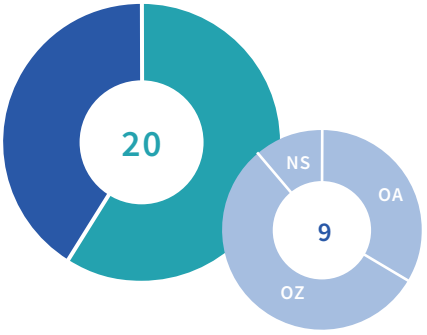
Classification level	2021	2022
RESTRICTED	2	9
CONFIDENTIAL	78	79
SECRET	11	25
TOP SECRET	3	1
Total	94	114

In 2022, the NSA issued 13 decisions, which were appealed against by **four** entrepreneurs.

In two cases, the NSA ruled in favor of changing the decision and two appeals were decided by the Committee which dismissed the appeals of the undertakings. At the end of the year, there was no appeal in the appeal process.

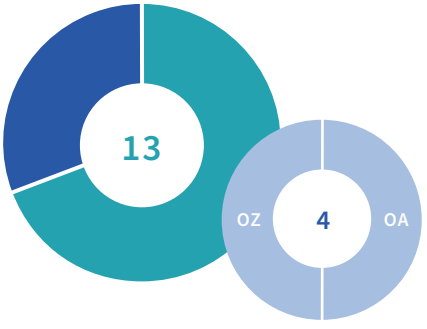
2021

9



2022

4



NSA's decisions, appeals by entrepreneurs against NSA's decisions and legal actions in 2021 and 2022

	2021	2022
DECISIONS OF THE NSA	20	13
APPEALS	9	4
Appeals – self-reversion (OA)	3	2
Appeals dismissed by the Committee (OZ)	5	2
Decisions cancelled by the Committee (RZ)	0	0
Legal Actions brought before the Supreme Court (SC)	1	0

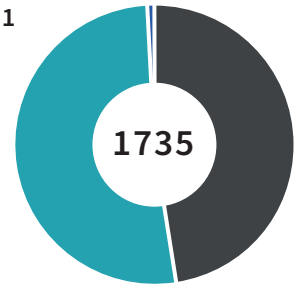
In relation to NATO and EU classified information, the NSA issued **6 NATO certificates and 3 EU certificates** to entrepreneurs, which entitle entrepreneurs to become acquainted with NATO classified information or EU classified information.

SECURITY OF INFORMATION

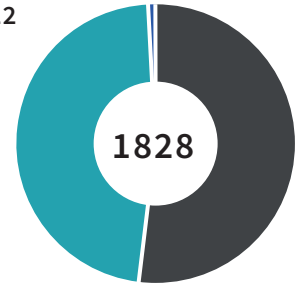
In 2022, the National Security Authority received and sent **1 828 classified documents.**

Data on classified information exchanged in the internal environment - internal inter-departmental communication – are not mentioned in the total number of 1 828. Since 2022, the electronic information system for the management of the registry allows the creation of classified information of the classification level Restricted also in terms of content.

2021



2022



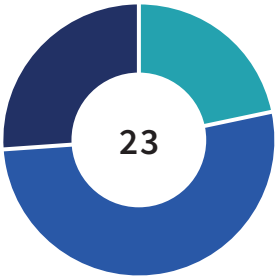
Classification levels of issued certificates

Classification level	2021	2022
RESTRICTED	826	950
CONFIDENTIAL	898	867
SECRET	11	11
TOP SECRET	0	0
Total	1735	1828

PHYSICAL SECURITY AND BUILDING SECURITY

In 2022, the NSA issued **37 certificates** for mechanical prevention devices (MPD) and technical safeguarding devices (TSD).

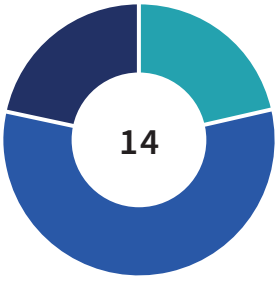
MPD



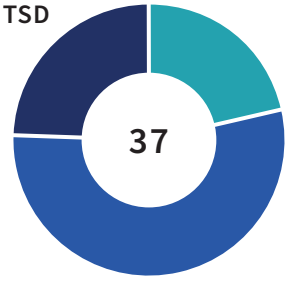
Classification levels of issued certificates

Classification level	MPD	TSD	MPD and TSD
RESTRICTED	0	0	0
CONFIDENTIAL	5	3	8
SECRET	12	8	20
TOP SECRET	6	3	9
Total	23	14	37

TSD



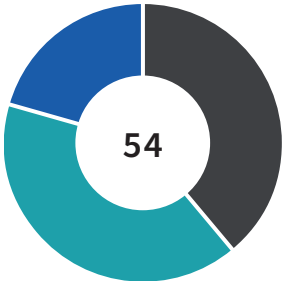
MPD and TSD



SECURITY OF TECHNICAL DEVICES

In 2022, the National Security Authority issued **54 certificates** of technical devices (TD) and **20 amendments** to already issued certificates of technical devices.

2021



Classification levels of issued certificates

Classification level	TP
RESTRICTED	21
CONFIDENTIAL	22
SECRET	11
TOP SECRET	0
Total	54

ACCREDITATION OF COMMUNICATION AND INFORMATION SYSTEMS

In 2022, the National Security Authority carried out **3 accreditations** of communication and information systems in accordance with the NATO Security Policy C-M(2002)49-REV1 and **2 accreditations** of communication and information systems in accordance with the Council Decision on the security rules for protecting EU classified information (2013/488/EU).

PROTECTION AGAINST UNDESIRABLE ELECTROMAGNETIC RADIATION

To ensure the protection of classified information against leakage through undesirable electromagnetic radiation, the Technical Department performed in 2022 zone measurements of protected areas (with mobile measuring equipment) and measurements of technical devices (TD) and means of cryptographic protection of information (MCPI) in the specialized TEMPEST laboratory.

In 2022, based on 35 requests received, the NSA performed 268 measurements of equipments (TD and MCPI) and 52 zone measurements of premises, on the basis of which **46 equipment components of technical means and 51 rooms** were categorized.

There were also adopted:

- 2 requests for shielded chamber attenuation measurements, which resulted in 5 measurements and assessment of 2 shielded chambers,
- 2 requests for attenuation measurements of shielded containers, which resulted in 4 measurements and 3 containers being assessed,
- 1 request for technical security inspections of premises, on the basis of which inspections of 12 rooms and 16 official vehicles were performed

BUILDING SECURITY AWARENESS

The National Security Authority conducts security officer's examinations and retraining of persons in the field of protection of classified information. Examinations and retraining are carried out in various areas of security, mainly in the form of online test in separate web application. Communication during the examination and retraining takes place in a virtual videoconference room.

In 2022, **431 candidates were invited** for the examinations. Of those invited, 284 candidates passed the examination (31 of them in attendance form and 34 within the Ministry of the Interior) and 78 candidates were unsuccessful (4 of them within the Ministry of the Interior of the Slovak Republic). The remaining number of candidates did not take part in the examination.

131 applicants were invited for retraining during the evaluated period . Out of this number of invitees, 113 candidates successfully completed the retraining (12 of them in the form of attendance and 14 within the Ministry of the Interior of the Slovak Republic) and 2 candidates were unsuccessful. The remaining number of applicants did not participate in the retraining.

In addition to the above activities, the NSA also issued 4 certificates of completion (duplicates) in 2022.

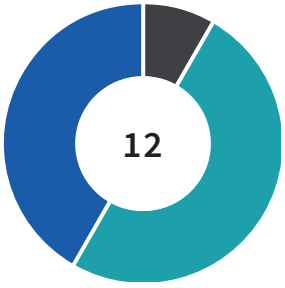
CRYPTOGRAPHIC PROTECTION OF INFORMATION

PERSONNEL SECURITY

The cryptographic protection system in the Slovak Republic is based on the verified structure of departmental cryptographic bodies and their close cooperation with the NSA, which fulfills the role of a central cryptographic body. The main areas of communication in 2022 were the certification of cryptographic protection of information (CPI) devices, the issuance of amendments to the rules on the use of CPI devices and questions about the possibilities of recognition and acceptance of foreign certificates.

For the year 2022, the NSA issued **12 certificates** of CPI devices and **7 amendments** to the already issued certificate.

2022



Classification levels of issued certificates

Classification level	TP
RESTRICTED	1
CONFIDENTIAL	6
SECRET	5
TOP SECRET	0
Total	12

SECURED INFRASTRUCTURE

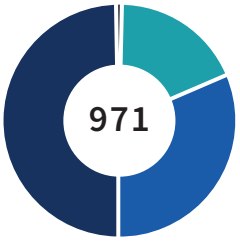
The National Security Authority continued to distribute devices designed to securely exchange information between government institutions in the mode of classification level Restricted, Confidential, and Secret. The NSA ensured the protection of videoconferences and transmission of information for members of the Government of the Slovak Republic.

The advancement of digital transformation in the conditions of public authorities and municipalities, together with the current security situation, causes a constant increase of requirements for services and support provided by the NSA in the operational environment of the systems for ensuring the defense and security of the Slovak Republic.

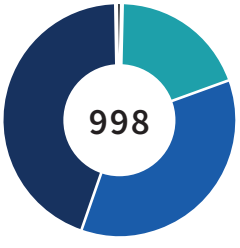
During 2022, the security and operational reliability of these systems have been improved by using new technologies of CPI devices. For the sustainability of the implementation of the set objectives the training of personnel was aimed at acquiring and developing professional competences for the management of information systems, competences ensuring the protection of information systems, web services, technical devices and CPI devices in the administration of the NSA.

In 2022, the National Security Authority directly operated 6 systems with CPI, operated or provided support for 433 end devices and provided services and support for 805 users in the conditions of the secure infrastructure of the Slovak Republic, with a total of 998 completed requests from these users during the assessed period. The NSA continuously ensured the operational requirements of the ministries and provided support in the production and distribution of cryptographic material.

2021



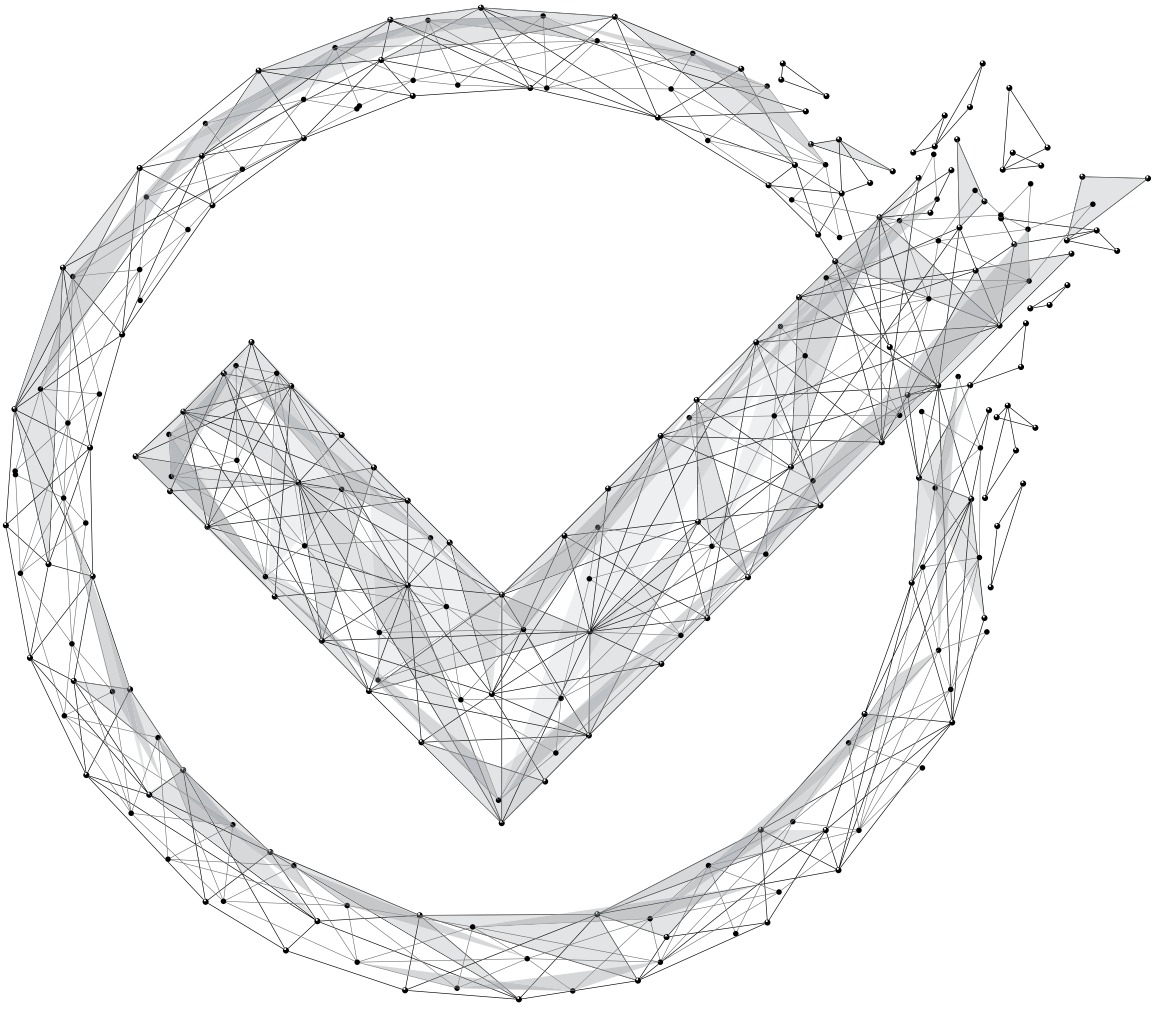
2022



Classification levels of issued certificates

Classification level	2021	2022
SYSTEMS	5	6
END DEVICES	360	433
USER ACCOUNTS	621	805
REQUESTS	971	998

TRUST SERVICES



In the course of 2022, the Council adopted a common position on the proposal for a revision of Regulation (EU) No. 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

The revision aims at universal access to secure and trustworthy electronic identification and authentication through a European digital identity wallet on a mobile phone, through which a person obtains his/her confirmation (electronic attestations of attributes) and can send only the necessary data from the confirmations to the relying party (e.g. car rental company) the relying party has provided at least the information necessary to authenticate access to the wallet. The Council proposes that the implementation period of 24 months counts from the adoption of the implementing acts.

At the level of the eIDAS Expert Group, the National Security Authority prepares the documents and actively participates in the work that will define the procedures also under Article 45d, where Member States will ensure that measures are taken, enabling qualified providers of electronic attribute certificates to verify the authenticity of those attributes by electronic means, at the request of the user, on the basis of a relevant authentic source at national level or through designated intermediaries recognized at national level in accordance with national or Union law, and in cases where those attributes are based on authentic sources in the public sector.

CERTIFICATION

In 2022, the Technical Department did not receive any request for certification of a secure product for qualified electronic signature. Qualified trust service providers use qualified electronic signature devices or qualified electronic seal devices already certified in another European Union member state and published in the list of devices certified by the European Union.

TRUST LIST

The National Security Authority maintains and publishes on its website a trust list containing information on qualified trust service providers that are under the supervision of the Slovak Republic and information on qualified trust services provided. During the year, the Authority published trusted lists No. 85 to 99.

LIST OF AUTHORISATIONS

The list of authorizations, which is an information source for qualified trust service providers for the issuance of mandate certificates, is published by the NSA on its website. On the basis of requests from state authorities and local government bodies, 18 new authorizations have been added to the list. During the year, the NSA published 9 versions of the list of authorizations. Its current version has always been supplemented by an archive of previous versions.

NEW TRUST SERVICES

The National Security Authority received notifications from five qualified providers with the intention to provide a qualified trust service. In total, fourteen qualified statuses for qualified trust service were conferred.

Two conformity assessment reports performed by a conformity assessment body within 24 months of the last audit were submitted to the supervisory authority by qualified trust service providers in 2022. They confirm that the qualified trust service providers and the qualified trust services they provide meet the requirements set out in the eIDAS Regulation. The NSA did not observe any breaches of security or integrity of the provision of trust services.

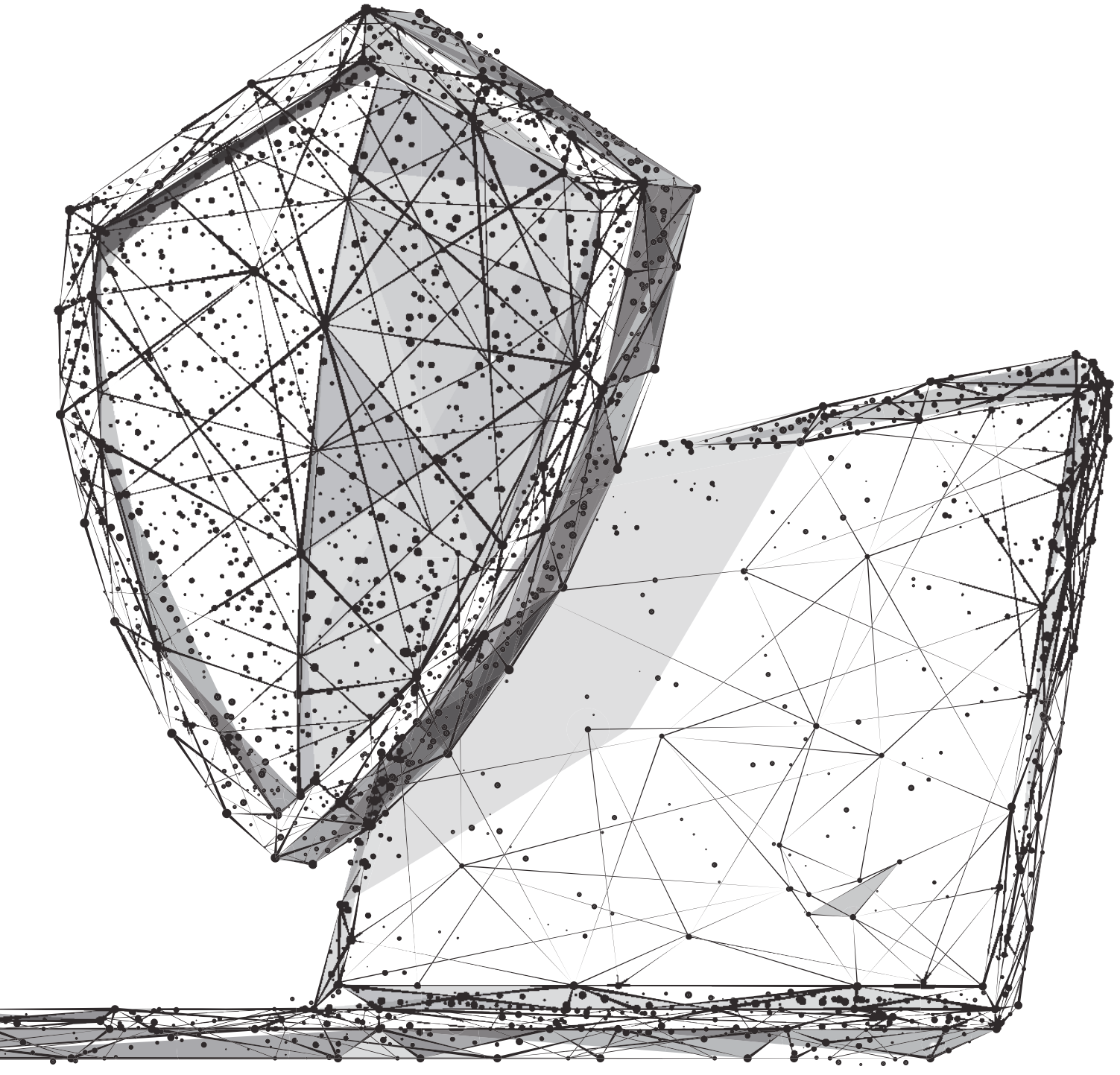
TRUST INFRASTRUCTURE

The National Security Authority operates a root certification authority of the Slovak Republic for the trust infrastructure, which issues public key certificates and maintains a long-term database of issued qualified certificates with their validity status, issued by providers to whom the NSA has granted qualified status. For the year 2022, a total of 122 357 certificates are registered.

DEVELOPMENT OF INTERNATIONAL STANDARDS

One NSA officer was project leader for the development of international technical standards used for the implementation of the eIDAS regulation (ISO 14533-1 within ISO TC 154). Work on the revision of ISO 14533-1 has been completed with its release in mid-2022.

CYBER SECURITY



The National Security Authority, through the National Cyber Security Centre SK-CERT, gathers reports of cybersecurity incidents, analyses, evaluates, supervises and coordinates their handling.

Its activities are carried out its in such a way that when cybersecurity incidents occur, the damage is remediated and minimized. At the same time, warnings are distributes and thus the level of prevention increases.

The activities of SK-CERT at the operational level in 2022 focused mainly on activities related to cybersecurity of operators of essential services, including critical infrastructure elements. In addition to the development of warning, the National Security Authority shared relevant information with partners on the basis of international cooperation and its own activities resulting from the analysis of reported and logged incidents.

Number of cybersecurity incidents reported to the National Security Authority in 2022 by sector

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Banking	10	24	19	9	16	13	13	6	10	5	2	4
Transport	0	1	1	0	1	0	3	0	0	0	2	0
Digital Infrastructure	0	2	1	0	0	1	1	0	0	0	1	1
Electronic Communications	1	0	3	2	1	1	0	1	0	2	0	3
Power engineering	1	1	0	1	0	2	1	0	0	0	0	0
Infrastructure of financial markets	0	0	0	0	0	0	0	0	0	0	0	0
Post office	1	6	8	7	5	1	1	0	0	0	2	1
Industry	0	0	2	0	0	3	0	0	1	1	1	0
Water and air	0	0	0	0	0	0	0	0	0	0	0	0
Public administration	27	35	23	25	21	26	19	19	39	30	23	41
Health care	9	3	1	5	4	10	4	2	7	3	3	1
Other	51	37	42	125	47	46	28	27	51	45	43	42
TOTAL	**100**	**109**	**100**	**174**	**95**	**103**	**70**	**55**	**108**	**86**	**77**	**93**

In 2022, the NSA gathered a total of **1,170 reports of cybersecurity incidents**, including **20 reports of Category I** serious cybersecurity incidents, **8 reports of Category II** serious cybersecurity incidents, and **7 reports of Category III** serious cybersecurity incidents.

SK-CERT also gathered 1135 voluntary reports.

This represents a 28% increase in reporting year-on-year, but the increase was mainly in the area of voluntary reporting.

Slovak cyberspace was significantly affected by Russia's war against Ukraine in 2022. At the beginning of the conflict and during the year, increased activity of various hacker groups was observed, supporting and carrying out malicious activities on behalf of the Russian Federation.

The groups coordinated through social media, particularly on the Telegram communication platform, which also contributed to the involvement of sympathetic public in the attacks.

The most visible were DDoS attacks aimed at denying access to various websites and services of various public institutions as well as private companies. These attacks were coordinated and also targeted at other EU and NATO Member States - their public institutions or other important targets.

The attacks were often in response to statements by public officials or to the approval of specific sanctions imposed on Russia. Selection of targets was inconsistent and ineffective at first, but over time, improvements in attackers' tactics, techniques and procedures were observed, which included the use of better tools, more careful target selection, rewards, including financial, for the best attackers, and so on.

In addition to war-related cyber-attacks, large-scale phishing campaigns have been observed that exploit the identity of postal and delivery services. The NSA has been observing this trend since 2020. Attackers are also exploiting the identities of banks, and their attacks are becoming sophisticated - they are not just using common communication tools such as email.

In their attacks, they often use the distribution of phishing content via SMS, social networks, phone calls or other communication services (e.g. WhatsApp, Facebook Messenger, etc.).

In 2022, phishing campaigns were also widespread, exploiting the identity of law enforcement agencies (police, Interpol, Europol), in which attackers called on victims to pay money to avoid fictitious criminal prosecution.

Ransomware has been dominated for several years to the spread of malicious code, whose purpose is no longer just to encrypt data and then demand a ransom, but also to exfiltrate (steal data in order to monetize it) and then blackmail (if you don't pay, I'll disclose it).

Ransomware attacks have often devastating effects on the data and infrastructure of affected organizations, especially those that underestimate the application of security measures (such as proper backups). Several different types of ransomware with varying degrees of sophistication or methods of data encryption and exfiltration have occurred in Slovak cyberspace. However, other forms of malicious code have also been observed, aimed at data and information extraction, botnet creation and other malicious activities of attackers.

In 2022 continued the trend of vulnerabilities and bad settings in various systems and services. This problem is present throughout the Slovak cyberspace, regardless of sector. Often, non-updated systems and services were observed to contain vulnerabilities that were months or years old. Such situations are caused by incorrect or no implementation of security measures that are mandatory for operators of essential services, including critical infrastructure elements.

During 2022, the National Cyber Security Centre SK-CERT issued security recommendations and warnings about vulnerabilities and threats. NCSC SK-CERT issued a total of **52 summary security bulletins and 271 security warnings.**

In total, it highlighted **628 vulnerabilities and threats**.

CYBERGAME

In 2022, the NSA organized a competition in the field of cybersecurity under the name CyberGame. The aim was to bring closer in an interesting and playful way topic of cybersecurity to the public and spread awareness of threats and ways to protect important data.

At the same time, the game was intended to motivate people to engage themselves to cybersecurity and identify talents in this area. CyberGame was designed for anyone – enthusiasts, specialists, students, teachers, public administration employees; regardless of age, gender, employment or education.

It lasted from 1 March to 10 May 2022 and an ordinary laptop and freely available tools from the internet were enough to join. CyberGame combined more than 50 technical and non-technical tasks. The game was divided into 4 branches – malware analysis, forensics, obfuscation and cryptography and OSINT.

Each branch contained several scenarios (stories), which increased during the game. In all scenarios several tasks logically overlapped. The principle of the game was to collect points for the so-called "flags". The one who got the most points won. If the player used help, his points were reduced. For completing the entire scenario was a bonus award. **1242 players** joined the game.

Overall winner, best player in the women's category and the best student won trip to malware laboratory in Montreal. Other competitors from the remaining categories won material prizes. CyberGame won the IT project award in 2022, the so-called Slovak IT Oscar.

INTERNATIONAL RELATIONS

The NSA actively participated in national and transnational activities – by participating in conferences, workshops, working groups and other events, to exchange experiences and practical knowledge.

Working groups and various other international formats at the level of the EU, NATO and OSCE were options for promoting the interests of the Slovak Republic in the field of cybersecurity and participation in the creation of strategic, legislative and methodological documents.

The NSA is the main contact point on the international level, which in practice meant broad cooperation with foreign partners and partner organizations, especially in the working groups of NIS Cooperation Group, CSIRT Network, CyCLONE and organizations Trusted Introducer and FIRST by exchanging experience, operational information when dealing with cybersecurity incidents and best practice.

The most important activities were the exchange of information and coordination within serious incidents with international overlap. The representative of the NSA was active in ENISA Management Board and ENISA Executive Board. The NSA represents the Slovak Republic in the area cybersecurity also in the OSCE.

Information sharing continued at the national level with relevant entities, especially between the NSA, Slovak Information Service, Military Intelligence, National Agency for Network and Electronic Services, Police Force and Ministry of Investments, Regional Development and Informatization of the Slovak Republic. In addition to exchanging relevant information important for ensuring the national cyberspace, we communicated with partners the strategic and conceptual issues.

We participated in international exercises focused on cybersecurity and cyber defense. At the national level, the NSA covered communication platform for operators of essential services. The aim was to share experience, to exchange recommendations and to comment legislative documents related to cybersecurity.

The NSA provided methodological assistance, consultations and guidance in implementing legal requirements especially for operators of essential services and digital service providers, but also for central authorities according to the law.

In the field of cybersecurity, the technical department accredits CSIRT units. In 2022, the NSA did not receive any application for such accreditation. The technical department cooperates with analytical security workplaces for the purpose of exchanging and sharing information on security incidents.

CYBER SECURITY COMPETENCE AND CERTIFICATION CENTRE

The Cyber Security Competence and Certification Centre (hereinafter referred to as the "Competence Center") is a contributory organisation and its primary mission is to assist in the public interest to fulfil the professional tasks of the National Security Authority as the founder in the field of cyber security, protection of classified information, cryptographic protection and trust services.

In the defined scope of activities, these are mainly the tasks of a national sectoral, technological and research centre in the field of cybersecurity, conformity assessment for various types of objects in the field of cybersecurity, application and comprehensive implementation of projects from the European Structural and Investment Funds, the Cohesion Fund and other financial instruments of the European Union.

The Competence Center, as an accredited conformity assessment body, certifies cybersecurity auditors and managers and integrated management systems. In the context of cybersecurity, it is accepted a combination of information security management systems according to ISO/IEC 27001:2013, together with IT service management systems according to ISO/IEC 200001:2018, business continuity management according to ISO 22301:2019 and quality management according to ISO 9001:2015.

The Competence Center has been granted accreditation decisions by the Slovak National Accreditation Service for all the above mentioned management systems and for the assessment of the professional competence of auditors and cybersecurity managers. As the only conformity assessment body in Slovakia, it covers all assessment objects and valid certification schemes relevant for cybersecurity.

Activities under the Cybersecurity Made in Europe brand are also a form of conformity assessment. Only qualified bodies authorised by the European Cyber Security Organisation (ECSO) are entitled to award this trademark. The Competence Center is one of the authorised partners granting the mark in Europe.

The brand builds awareness of the strategic value of cybersecurity companies and organisations that develop their business on the basis of trusted European values. As an industrial marketing tool, it also enhances reputation with business partners, investors and end-users.

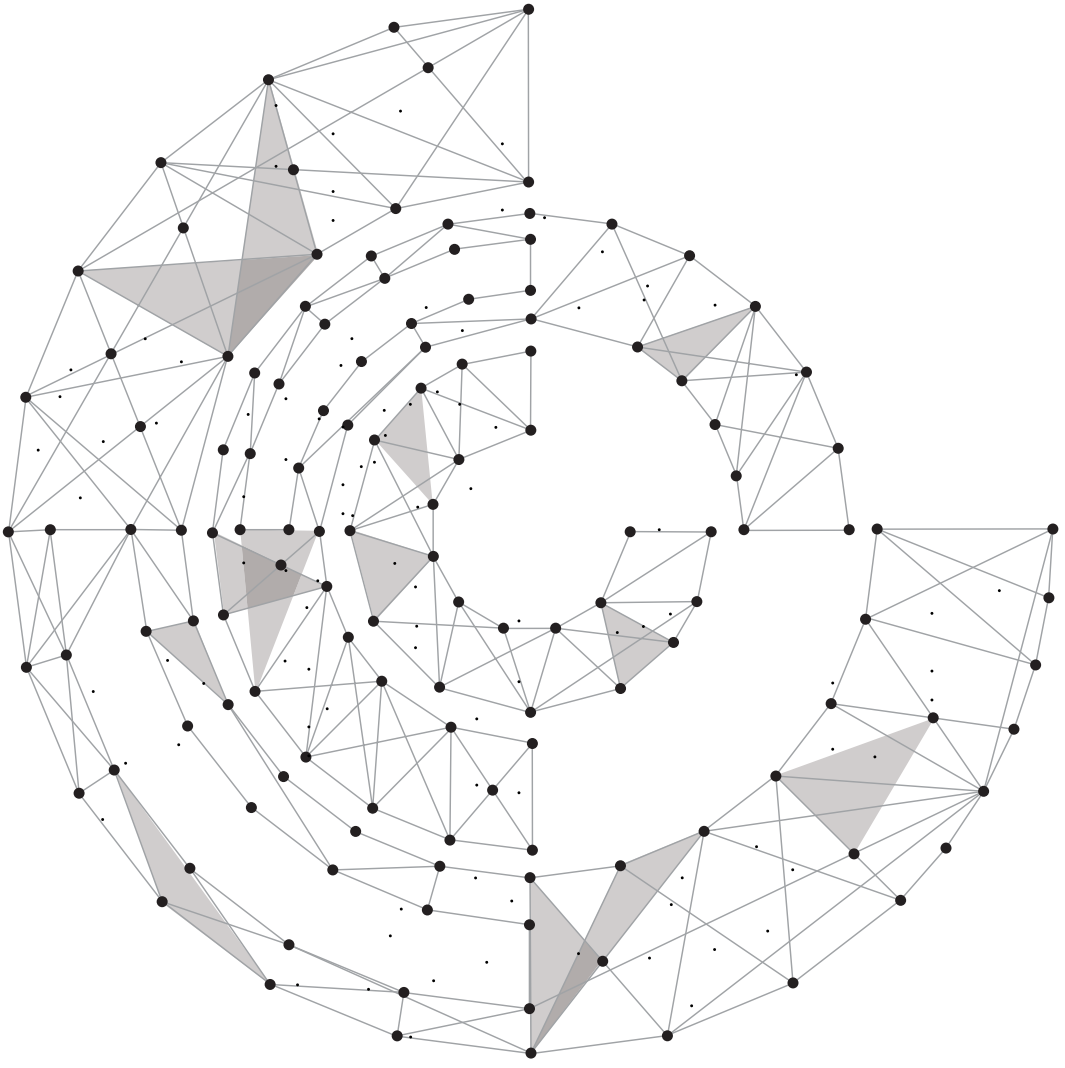
The Competence Centre also carries out cybersecurity audits of operators of essential services to confirm the effectiveness of the security measures taken and to verify compliance with the requirements laid down by law.

As a national sectoral, technological centre, the Competence Center acts mainly as an expert organisation on two levels – consultancy and expertise. Expertise is a specialised professional activity carried out by experts for the client, under the conditions laid down in the law. The acts of expert activity are mainly expert opinion and its supplement, professional opinion or confirmation, expert statement and explanation. Expert activities are carried out pursuant to Act no. 382/2004 on experts, interpreters and translators.

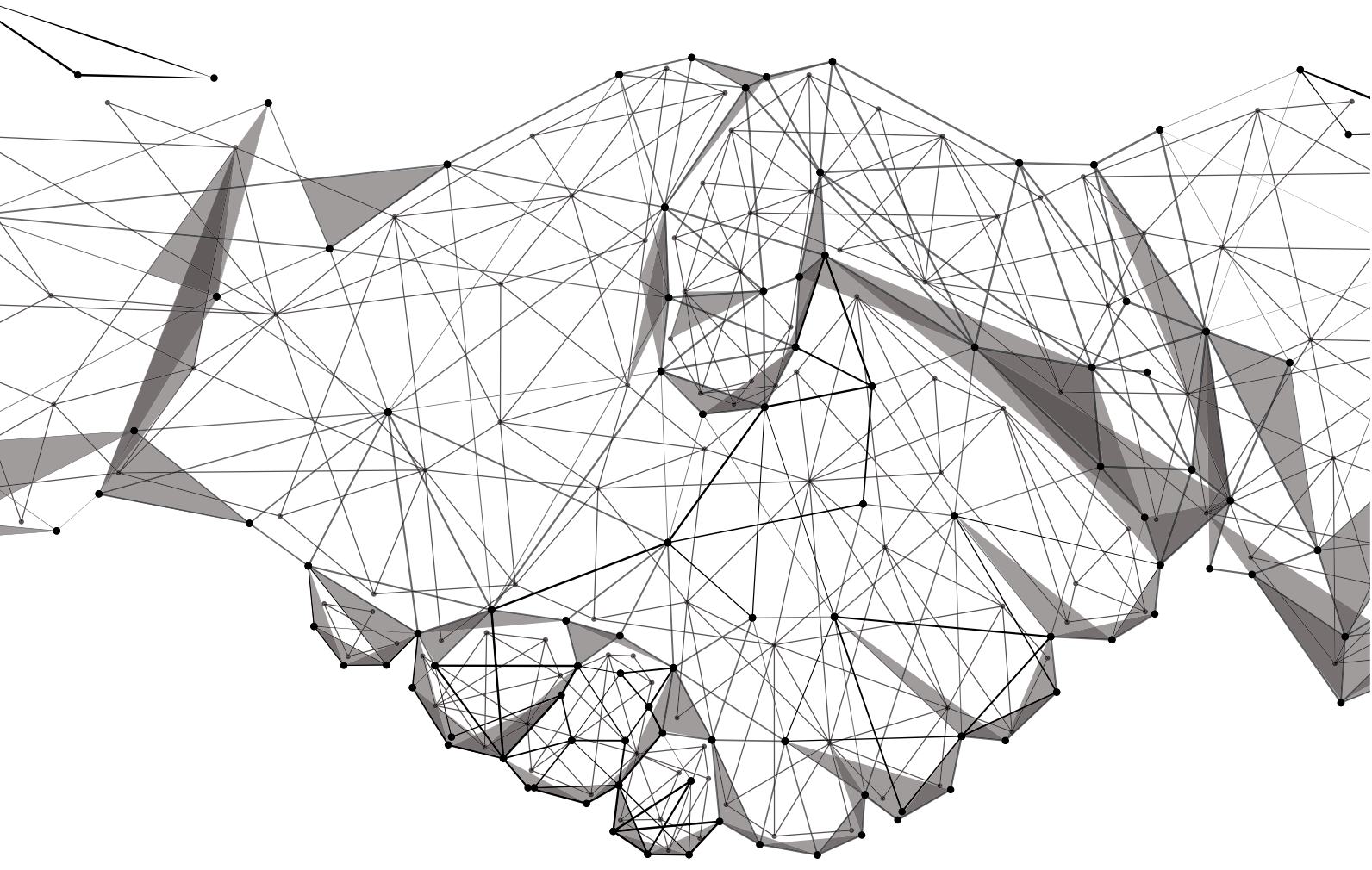
The main and indispensable role of the Competence Centre will be to implement relevant parts of the Digital Europe and European Horizon programmes by awarding grants and supporting public procurement. Funding resources for cybersecurity will be decided by the European Competence Centre in close cooperation with the network of National Coordination Centres and with community partners such as researchers, supplier and customer industries and the public sector.

The Competence Center has signed Memoranda of Cooperation with the absolute majority of relevant university workplaces that provide study programmes and courses in the field of information protection.

Last but not least, the task of the Competence Center is to educate adults in information and cybersecurity, including security awareness campaigns.



INTERNATIONAL COOPERATION

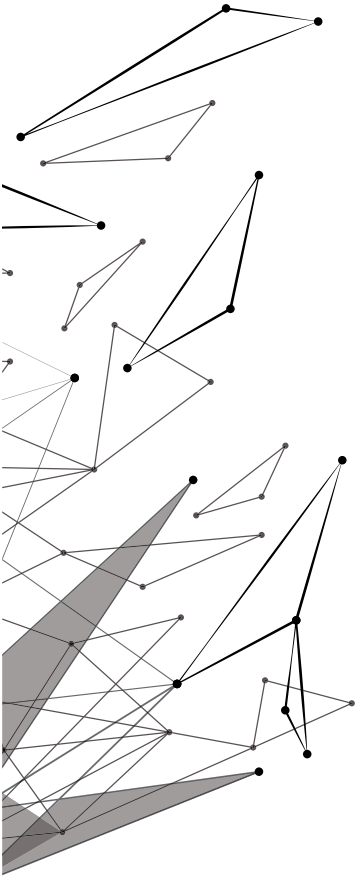


The covid 19 pandemic in 2020-2021 and the Russian invasion of Ukraine have significantly accelerated the development of the digital era. Digital technologies have become an essential part of everyday and professional life, and face-to-face contacts have become much more limited. This situation had a significant impact on the uptake of these technologies in practice and the related security challenges.

Last year, the NSA confirmed its direction in building a security environment that is in line with the principles adopted in the EU Security Union Strategy for the period 2020 – 2025 and the EU Cybersecurity Strategy for the Digital Decade.

Increasing the resilience of cyber infrastructure, cybersecurity and setting up processes to ensure security, both in the physical and digital environment, remain priorities.

As regards the development of the NSA's international relations, officers developed them on permanent international representation of the Slovak Republic, where they participated and contributed to the development of security policies in the EU and NATO. They also developed international activities, bilateral relations and regional cooperation.



EUROPEAN UNION

The NSA officers participated, in person or virtually, in regular meetings of the Security Committee of the Council of the EU (CSC), the European Commission's Security Policy Expert Group (ComSEG) and the Security Committee of the European External Action Service (EEAS).

In 2022, work continued at the EU Council on the revision of the security rules to eliminate the shortcomings identified in application practice and to increase the comfort for the addressees of these rules. In the working formats mentioned above, the NSA was actively involved in the preparation of security standards in order to enhance the level of protection of classified information and continued to be actively involved in the process of revision of the security rules.

A major revision of the Council's security rules for the protection of EU classified information (EUCI) is currently under way. The NSA has therefore been actively involved in the development and revision of the rules in the area of personnel and industrial security. Discussions also continued on changes to the exchange of EU classified information with third countries and international organisations, as well as on the Proposal for a Regulation of the European Parliament and of the Council (EU) establishing a Union Secure Connectivity Programme for the period 2023-2027 (EU Secure Connectivity Programme).

However, the most discussed topic was the forthcoming EC Regulation on common rules for the protection of EU classified information for all EU institutions, bodies and agencies. Member states agree that the legal basis for all EU security rules is laid down by the Council in valid documents. At the regular meeting of the Security Committee of the European External Action Service (SC EEAS), EEAS officers participated in the revision of the security awareness programme and the intensification of staff training on possible cyber risks. In this context, a manual is being prepared to help not only for newcomers

in working with EUCI. EEAS staff have contributed to building resilience and security awareness in EU Delegations abroad through training, workshops and outreach programmes.

The NSA was regularly and actively represented at the meetings of the Horizontal Working Party on Cyber Issues (HWPCI) during the French and Czech Presidencies of the Council of the EU. In the legislative field, 2022 was an important milestone for strengthening EU cybersecurity.

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 (NIS 2 Directive) has been adopted.

The main task of the NSA in this regard will be its transposition into national legislation. Another important and follow-up step was the presentation of the draft legislation on cyber resilience, which sets out the cybersecurity requirements for products with digital elements. A crucial task in this respect will be to set clear rules to ensure a high level of EU cybersecurity, with a vision of setting standards for the rest of the world as well.

The HWPCI meetings also dealt with the negotiation of non-legislative documents. The most important of them are the Strategic Compass, the EU Council Conclusions on the development of the EU's cyber posture, the Council Conclusions on ICT supply chain security and the proposal for a new cyber defence policy presented in the EC's so-called defence package.

The area of cyber diplomacy has been greatly affected by events in the EU's eastern partner. Therefore, the HWPCI deliberations also focused on the formulation of the texts of the EU High Representative's statements of condemnation of the cyber-attacks by Russian actors to Ukraine that preceded and persisted during Russia's invasion. In this context, the issue of revising the cyber diplomacy toolbox (CDT) has been raised several times.

At the European Union Agency for the Space Programme (EUSPA), the development of Programme Security Instructions (PSIs) was a major point of discussion. These extensive documents have been prepared in the various supporting working groups, e.g. Galileo Security Working Group, GOVSATCOM, Copernicus or Egnos.

New EC initiatives have been created in the context of the GOVSATCOM programme. This is the EuroQCI (Quantum Communication Infrastructure) ad hoc group, which contributes to the discussion on the cross-cutting theme of quantum communication infrastructure. It is to be used in the context of the GOVSATCOM programme to ensure a high level of encryption, resilience and, last but not least, security. This network is also to be adapted for the transmission of classified information.

The key priorities of the Cooperation Group continue to be the implementation of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of network and information systems security in the European Union (NIS Directive) and the related application of the individual instruments.

In 2022, other important topics such as "Risk assessment and risk scenarios", which also follows from the task for the Cooperation Group and is addressed in the Council Conclusions for the development of an EU cyber posture, "Crisis management", "Organisation and potential areas for future cooperation in the Cooperation Group" and "Coordinated vulnerability disclosure" have been added to this task. ENISA conducted a roadmap of needs for cybersecurity exercises and member states shared their experiences on the most serious cybersecurity incidents and threats that affected them during the year (ransomware dominated again).

Work Stream 3

A group focused on the notification obligations of operators of essential services. As part of its work, the group has been dedicated to improving the individual tools that serve for notification obligations for Member States.

Work Stream 7

a large-scale cybersecurity incident response group. At the level of this group, the development of operational procedures for dealing with serious incidents with an international dimension has continued and representatives of the NSA have actively participated in them.

Work Stream 10

Digital Infrastructure Group. At the platform, Member States dedicated to the competent authorities and their obligation to define and follow a common approach to implementation requirements for digital service providers (DSPs). The intention of the NIS Directive was to define a maximum harmonisation framework for DSPs, which will be subject to the jurisdiction of a single competent authority (the competent authority in the country of their head office in the EU) for all their activities in the Union.

Work Stream 5G

Group for security and protection of G security. The EC has published a set of recommended measures to mitigate the risks associated with the construction and operation of 5G networks, the 5G Toolbox. The application of these measures has also been transferred to the national level, in particular in the form of application practices.

Work Stream 12

security measures in the given segment), which takes a realistic form. Another objective is to increase the cybersecurity measures of entities that fall within the healthcare sector.

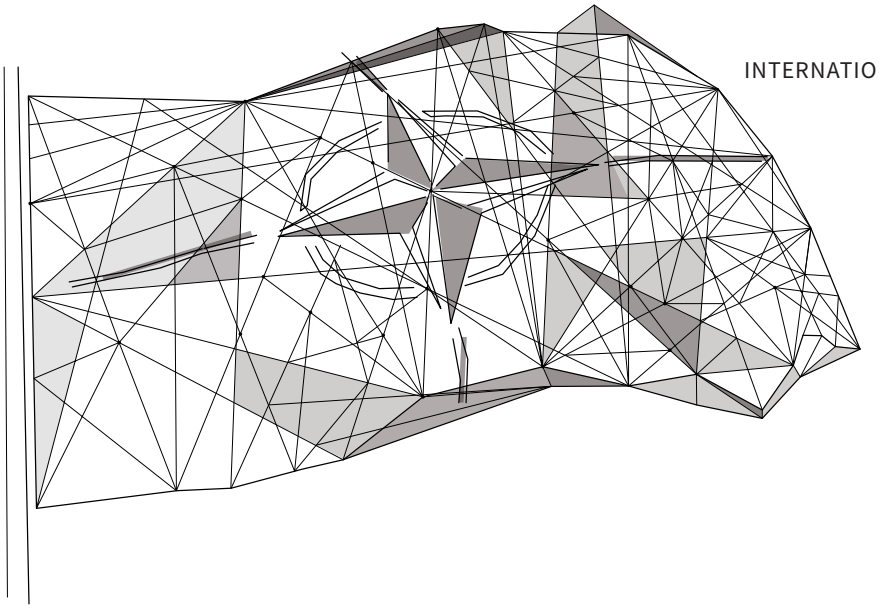
Work Stream 15

During 2022, the newly established Work stream 15 – Supply Chain Security Group focused on strengthening ICT supply chain security and taking the first steps to address the threat of unwanted strategic dependencies in ICT supply chains.

EU CyberNet

During the year, the EU Cyber-Net community, which brings together national authorities and institutions working in the field of cybersecurity, expert groups in the field, think- tanks and academic institutions based in EU Member States, also gained importance.

EU CyberNet organised a number of workshops and conferences during the year that were dedicated to current topics of cybersecurity issues, where the NSA officers increased their expertise and knowledge by actively participating in these activities and building the capacity of the NSA.



NATO

NATO has been greatly influenced by geopolitical developments, especially the situation in Ukraine. Cyber attacks carried out by Russian actors, which preceded the unprovoked invasion itself and which continue to persist, have been condemned by NATO Secretary-General Jens Stoltenberg in public statements.

The Cyber Defence Committee (CDC) has been extensively engaged in providing assistance to the war-affected partner and expediting its entry into Cyber Defence Centre of Excellence in Tallinn.

The war in Ukraine has also brought some lessons from the uncoordinated approach to providing assistance, and in this context the Madrid summit in July has produced an agreement by the allies to establish a virtual cyber rapid response unit, which would voluntarily bring together cyber experts to work together in response to serious malicious cyber activities.

In 2022, the first meeting of National Cyber Coordinators was held at the North Atlantic Council (NAC). The main topic of discussion was national cyber defence contributions to the overall alliance deterrence and defence forces in response to events in Ukraine. The Director of the National Cyber Security Centre SK-CERT attended the meeting on behalf of the Slovak Republic.

The NATO Security Committee (SC) continued to meet in all its formats - Security Policy, Communications and Information Systems Security (CISS) and at the highest level - the level of the directors of the security authorities of the member states.

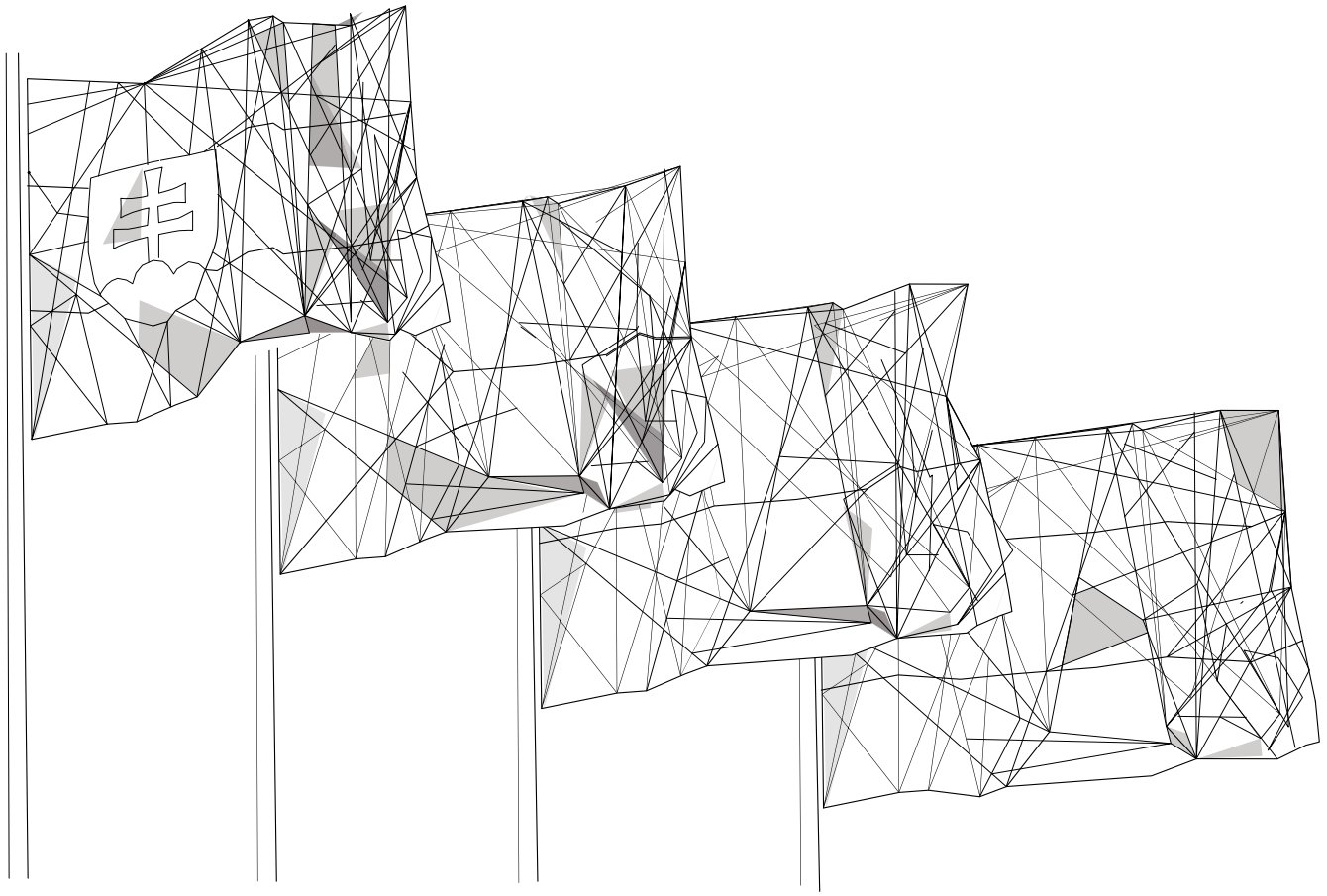
This year was marked by the continuation of a major revision of NATO security policy in terms of the protection of classified information. The NSA representatives also participated in a meeting of an expert group of specialists from member states on industrial security (Capability Team) and during the October meeting presented to the NATO Security Office (NOS) and the delegates the proposals to amend the Directive on Classified Projects and Industrial Security.

The Communications and Information Systems Security format of the NATO SC addressed two main documents - the Cybersecurity Directive and the NATO Strategy on Artificial Intelligence (AI). During the October meeting at the highest format (Principals level), the agenda for 2023 was presented to the participants.

In March, the NSA officers participated in the NATO CMX crisis management exercise (an exercise at the highest strategic level aimed at practising and improving political consultation and decision-making). Its purpose was to practise the implementation of the measures of the National Crisis Response System. The NSA was involved in the management, coordination, monitoring and evaluation of the course of exercise and his evaluation.

The NSA also participated in the joint alliance exercise NATO Able Staff 2022 that took place in December 2022 to test communication procedures related to nuclear planning, to practice applicable measures of the Alliance's crisis response system, to bring improvements in the consultation area, to conduct practical training of personnel at NATO Headquarters, Supreme Headquarters Allied Powers Europe (SHAPE) and at national headquarters.

The NSA participated in the exercise at the distribution level, ensuring the receiving and transferring of classified information through the Central Registry. Communication during the exercise was via the NS WAN and NNCCRS (NATO Nuclear Command Control Response System) information system, which was used for the flow of information between the involved ministries, the NSA and NATO Headquarters.



REGIONAL COOPERATION

The NSA represented Slovakia by chairing the Central European Cyber Security Platform (CECSP). The countries of the Visegrad Four (Czech Republic, Hungary, Poland, Slovak Republic) and Austria have their experts in the CECSP.

The NSA organised a workshop in a physical format on 12 September 2022 in Bratislava, which was highly appreciated by partner. It focused on current issues that resonated at EU level. Among the most important were the transposition of NIS 2 and the coordination of vulnerability reporting.

The Slovak Republic has become visible by the presentation on the topic of the location of the competence centre in the system of cybersecurity regulation. NSA officers also presented a concept for the cybersecurity community.

A comprehensive study on the cybersecurity audit in Slovakia was presented by the representative of the Competence Centre. Experts exchanged mutual knowledge and gave examples of good practice in transposition of the NIS 2 Directive.

BILATERAL RELATIONS

The NSA developed bilateral relations across all working platforms.

Slovakia and the United States of America signed a bilateral agreement concerning security measures for the protection of classified information. It significantly contributes to deepening relations and intensifying cooperation between the two countries.

During the year, we started negotiations on a similar agreement with the Netherlands.

The expansion of the sphere of cooperation has also focused on East Asia. We received two foreign visits from the Republic of Indonesia. The delegations were interested in the area of protection of classified information and cybersecurity.

Closer cooperation was established in both segments in order to conclude international agreement on the protection of classified information and Memorandum of Cooperation in the field of cybersecurity.

In September 2022, a delegation from North Macedonia visited Slovakia during the European TAIEX programme. NSA officers prepared several presentations and educational activities, in particular on the requested topic of physical and building security.

At the end of 2022, the Government of the Slovak Republic concluded a security agreement with the European Space Agency (ESA).

Meetings with the Czech National Cyber and Information Security Agency (NÚKIB) have also intensified. The meetings focused mainly on the adaptation of national certification procedures and legislation to the forthcoming pan-European system of certification schemes.

EXCHANGE OF FOREIGN INFORMATION

The electronic registration of foreign classified information through online links with public information registers enables secure, faster and more flexible registration and electronic distribution of classified information.

In 2022, the NSA continued to provide methodological assistance to the electronic registry of classified information set up by public authorities in the electronic registration of classified information. The Central Registry Office processed **4 218 NATO classified information and 2 522 EU classified information.**

The NSA also mediated the exchange of **160 classified information of foreign power**. The NSA has created an established register of NATO ATOMAL classified information since 2010. No ATOMAL classified documents were registered in 2022.

In connection with the entry into force of Act No 364/2020 amending Act No 395/2002 on archives and registers, the National Security Authority has established a central storage facility for the temporary storage of classified information of permanent documentary value since 2021.

The central storage for classified information is set up at the detached workplace in Topoľčianky.

Priorities for 2023 continue to launch of the integration of the electronic registry management information system with the external environment.

Classification level	2021	2022
NATO — RESTRICTED	1739	1833
EU — RESTRICTED	693	886
FOREIGN POWER — RESTRICTED	48	114
NATO — CONFIDENTIAL	732	568
EU — CONFIDENTIAL	486	750
FOREIGN POWER — CONFIDENTIAL	49	39
NATO — SECRET	1209	1770
EU — SECRET	346	886
FOREIGN POWER — TAJNÉ	3	7
NATO — TOP SECRET	0	0
EU — TOP SECRET	0	0
FOREIGN POWER — TOP SECRET	3	0
NATO — TOTAL	**3680**	**4218**
EU — TOTAL	**1525**	**2522**
FOREIGN POWER — TOTAL	**103**	**160**

ECONOMY

Schedule of commitment appropriations for the budget of Chapter 41 – The National Security Authority for 2022, the impact of budgetary measures on the level of the adjusted budget, the actual implementation of budget to 31 December 2022 and the percentage assessment of the implementation in relation to the adjusted budget are presented in Table 1

The binding indicators of the Authority's budget for 2022, approved by Law No 534/2021 on the State Budget for 2022, have been respected by the Authority. In the management with the financial resources the NSA proceeded according to the principles of economy, efficiency and expediency in compliance with the legislative regulations, in particular Act No. 523/2004 Coll. on Budgetary Rules of the Public Administration, Act No. 357/2015 Coll. on Financial Control and Audit, Act No. 343/2015 Coll. on Public Procurement, resolutions of the Government of the Slovak Republic and methodological instructions and guidelines of the Ministry of Finance of the Slovak Republic.

BUDGET FOR 2023

The binding indicators of the state budget of the individual chapters for 2023 were approved by Act No 526/2022 Coll. on the state budget for 2023. Following point C.1. of the Government Resolution No 636 on the draft budget of the public administration for the years 2023 to 2025 and the provision of Article 6(3) of Act No 523/2004 Coll. on the budget rules of the public administration, the binding indicators of the state budget for 2023 were notified to the Authority.

The expenditures of NSA for 2023 are budgeted in programme 0D9 – Information Security and inter-ministerial sub-programme 0EK0U – Information Technology financed from the state budget – NSA in the total amount of EUR 14,612,255.00. The NSA's revenue as a binding indicator is budgeted at EUR 20 000,00, revenue under source code 72e is budgeted at EUR 2 000,00.

The Authority will use the budget funds in the performance of tasks arising from its status as a central state administration body for the protection of classified information, cryptographic service, cybersecurity and trust services. Other tasks of the NSA are related to the fulfilment of tasks from the resolutions of the Government of the Slovak Republic and result from the obligations of the Slovak Republic towards the EU and NATO.

PUBLIC PROCUREMENT

Analysts from the Transparex.sk portal have compiled in 2022 a ranking of "Responsible public procurers for 2021". The ranking consisted of all state organisations – cities and municipalities, regions, central state administration bodies, hospitals, state-owned enterprises, kindergartens and schools. The National Security Authority ranked 2nd with an overall ranking of 87.16 points and a grade of A+, which means "very responsible procurer".

In the ranking of the category "Central Government Bodies", the National Security Authority was ranked 1st.

NATIONAL CULTURAL MONUMENT – MANOR HOUSE BRUNOVCE

The National Security Authority has in its administration a renaissance manor house from the second half of the 17th century located in the village of Brunovce, Nové Mesto nad Váhom district. The manor house is registered in the Central List of Monuments, in the real estate register of national cultural monuments. There is an English park around the manor house from the end of the 18th century.

Until the outbreak of the covid pandemic, the manor house was accessible in limited extent to the local community and the general public, and at the same time it was used mainly for official purposes as a training centre, but also for various private events of the NSA staff and also for other citizens for the purpose of accommodation or renting rooms and exteriors of the manor house (e.g. wedding photography, celebration of the anniversary of the village and the associated holy mass in the chapel of the manor house).

Due to the unsatisfactory technical condition of this national cultural monument, in 2022, the authority proceeded to the plan of its complete restoration. The main objective is to obtain funding from the priorities of the National Recovery and Resilience Plan for the restoration of public historic and listed buildings.

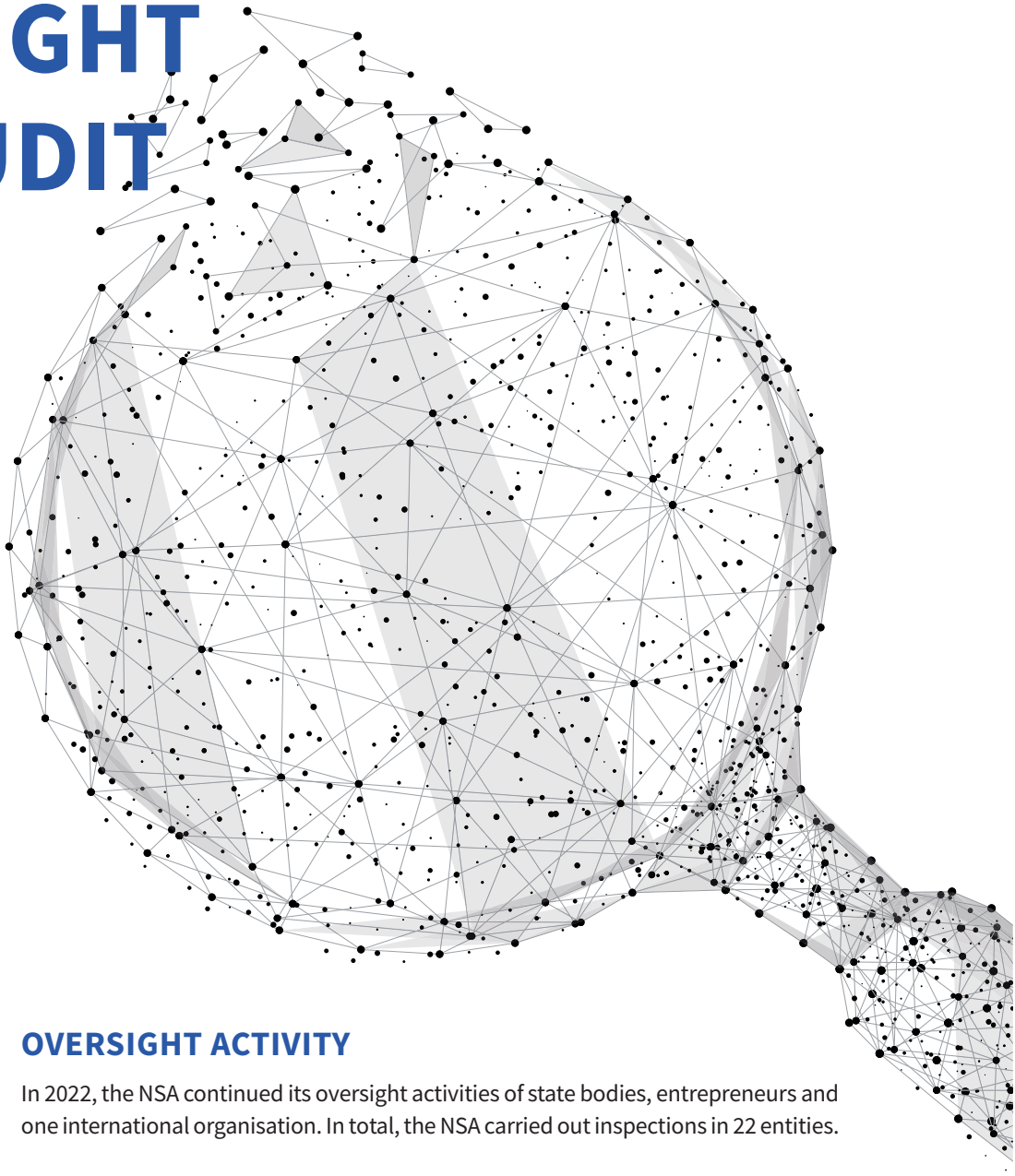
The reconstruction will be focused primarily on improving the energy efficiency of the manor house activities related to the construction and engineering restoration and implementation of green measures with the aim to prolong the lifetime and the possibility of wider use of this national cultural monument.

Table 1: Budget of the National Security Authority in 2022 (in euros)

*number of employees as of 31.12.2022 (excluding maternity and parental leave)

INDICATORS	APPROVED BUDGET	ADJUSTED BUDGET	REALITY K 31. 12. 2022	FULLFILLMENT TO THE ADJUSTED BUDGET
I. Revenues of the chapter	**20 000,00**	**20 000,00**	**38 424,22**	**192,12%**
A. Mandatory indicator	20 000,00	20 000,00	38 424,22	192,12%
B. Funds from the European Union	0,00	0,00	0,00	
II. Total expenses of the chapter (A + B+ B+ C + C.1)	**12 844 288,00**	**14 474 812,33**	**13 885 343,39**	**95,93%**
A. Total expenses excluding funds according to art. 17(4) of the Act No 523/2004 Coll. and funds from the European Union	**12 842 288,00**	**14 436 307,40**	**13 846 838,46**	**95,92%**
out of that:				
A. 1. budgetary funds from chapter	12 842 288,00	14 424 566,63	13 835 097,69	95,91%
out of that: source code 111 + 11H + 11UA	12 842 288,00	13 353 915,99	13 065 873,33	97,84%
Source code 131	0,00	1 070 650,64	769 224,36	71,85%
A. 2. funds for co-financing	0,00	11 740,77	11 740,77	100,00%
out of that: source code 3AA2	0,00	6 313,99	6 313,99	100,00%
source code 3AA3	0,00	5 426,78	5 426,78	100,00%
A. 3. wages, salaries, services income. and others personal. compensation (610), (source code 111 + 11H)	6 494 929,00	6 707 686,00	6 491 911,86	96,78%
out of that: wages, salaries, services income, wages, and other personnel. settlements of the central body				
(source code 111 + 11H + 11UA)	6 494 929,00	6 707 686,00	6 491 911,86	96,78%
Number of budgetary organisation employees according to Annex 1 to the Government Resolution No. 577/2021	250 osôb	254 osôb	214 osôb*	84,25%
out of that: apparatus of the central body	250 osôb	254 osôb	214 osôb*	84,25%
the administrative capacity of budgetary organisations in particular				
monitored according to Annex No. 1 to Government Resolution No. 577/2021	0 persons	0 persons	0 persons	
out of that: apparatus of the central body	0 persons	0 persons	0 persons	
A. 4. capital expenditures (700) (excluding the funds for co-financing)	250 000,00	1 343 795,81	1 042 369,53	77,57%
out of that: resource code 111	250 000,00	273 145,17	273 145,17	100,00%
source code 131I	0,00	240 665,88	108 665,88	45,15%
source code 131J	0,00	431 382,36	261 956,08	60,72%
Source code 131K	0,00	368 360,00	368 360,00	100,00%
source code 131L	0,00	30 242,40	30 242,40	100,00%
A.5. Recovery and resilience plan – VAT reimbursement funds	0,00	0,00	0,00	
B. Funds according to Article 17(4) of Act No. 523/2004 Coll. (According to § 17 (4) of Act No. 523/2004 Coll., the budgetary organisation is entitled to draw this limit up to the amount of the budget. revenue actually received and is entitled to exceed the expenditure in order to achieve higher than budgeted revenue.)	**2 000,00**	**2 725,70**	**2 725,70**	**100,00%**
C. Funds from the European Union	**0,00**	**35 779,23**	**35 779,23**	**100,00%**
out of that: source code 3AA1	0,00	35 779,23	35 779,23	100,00%
C.1 Funds from the Recovery and resilience plan	**0,00**	**0,00**	**0,00**	
D. Expenses of the state budget for the implementation of the programmes of the Government of the Slovak Republic and parts of the programmes of the Government of the Slovak Republic	**12 844 288,00**	**14 474 812,33**	**13 885 343,39**	**95,93%**
0D9 Information security	12 657 784,00	14 308 694,33	13 733 505,30	95,98%
0EK0U Information technologies from the state budget - NSA	186 504,00	166 118,00	151 838,09	91,40%
E. Systemisation of police officers in civil service	**228 osôb**	**232 osôb**	**192 osôb***	**82,76%**
	5 905 472,00	**6 111 867,00**	**5 963 241,23**	**97,57%**

OVERSIGHT AND AUDIT



OVERSIGHT ACTIVITY

In 2022, the NSA continued its oversight activities of state bodies, entrepreneurs and one international organisation. In total, the NSA carried out inspections in 22 entities.

Pursuant to Act No. 215/2004 Coll. on the protection of classified information, 10 entities were inspected, with various combinations of the following areas being the subject of the inspection: protection of classified information (9 times), cryptographic protection of information (2 times) and control of compliance with measures (1 time).

Oversight of obligations arising from NATO membership was carried out in one entity, and cybersecurity oversight was carried out in 11 entities.

In particular, the control teams focused on the complexity of the measures taken and their coordination across the individual security areas. Deficiencies were found in fourteen inspected subjects. The control teams recorded a total of 62 control findings in 2022:

- 51 in the field of cybersecurity,
- 0 in the field of physical and building security,
- 3 in the field of security of technical means,
- 5 in the field of personnel security,
- 3 in the field of security of information.

METHODOLOGICAL ACTIVITY

The Security Council of the Slovak Republic adopted a set of proposed measures for the current security situation (war in Ukraine) at its 145th session on 2 February 2022 in order to ensure reliable coordination of measures to maintain the security of the state and prevent crisis situations. The NSA was given the task of coordinating activities in the field of protection of classified information. In this context, the Authority has drawn up a list of the following measures for the affected entities, including the method of solving them:

- Increase the level of security clearance carried out for key persons,
- update procedures for the protection of classified information in the event of an emergency situation and crisis situation,
- to ensure that classified information is properly protected when handled and stored by the Head,
- to update the lists of classified information,
- to ensure the connection of the central register of classified information with the departmental registers by means of emergency services.

In the field of **regulation and methodology**, the Authority issues opinions and methodologies (methodological guidelines) to generally binding legal regulations and documents within the competence of the Authority, prepares proposals for generally binding legal regulations for the legislative process, comments and develops opinions on draft legislative materials in the **interdepartmental comment procedure** (the Regulation and Supervision Department registers 527 comment procedures dealt with in terms of its substantive competence, which does not include the interdepartmental comment procedures dealt with by other departments, as well as requests for sub-statements addressed to the Regulation and Supervision Department).

The NSA provides methodological guidelines to state bodies, natural and legal persons in all areas of its competence. The Authority also publishes anonymised methodologies and expert opinions on the Authority's website.

The Authority issued **157 guidance documents in 2022:**

In the field of protection of classified information	
PERSONNEL SECURITY	**37**
SECURITY OF INFORMATION	**7**
INDUSTRIAL SAFETY	**18**
PHYSICAL SECURITY AND BUILDING SECURITY	**6**
SECURITY OF TECHNICAL MEANS	**2**
SECURITY OFFICERS	**1**
AERIAL PHOTOGRAPHY	**5**
FOREIGN POWER	**9**
In the field of cryptographic protection of information	1
In the field of cybersecurity	21
In the area of trust services	15
Cross-sectional opinions	35
Total	85

SUPERVISORY ACTIVITY

In 2022, the Authority carried out supervisory activities to ensure, through ex ante and ex post supervision, that qualified trust service providers and the qualified trust services provided by them comply with the requirements set out in Regulation (EU) No. 910/2014.

Supervisory activities included in particular the analysis of conformity assessment reports for the regular 24-monthly audits and the process of granting qualified status, reporting obligations of qualified trust service providers for changes in the provision of qualified services, supervision carried out on the basis of complaints from external entities, checking whether they provide services for which they have not been granted qualified status, and checking compliance with national legislation in the area of trust services.

Conformity assessment reports from four qualified trust service providers were analysed in the preliminary supervision. Eighteen qualified statuses for qualified trust service were granted.

In the **subsequent supervision**, the conformity assessment reports were analysed, i.e. the received regular 24-monthly audit reports from three qualified trust service providers and two control audit reports from two qualified trust service providers.

INTERNAL CONTROL

The Authority's internal control body carried out 12 internal controls in 2022. Four of the controls concerned the substantive implementation of the government resolutions. The other controls focused in particular on checking adherence to the specified work hours of the officers and staff of the NSA, checking compliance with the obligations arising from the internal rules on the operation of service vehicles, the allocation and registration of service weapons and ammunition, other tactical material, checking service cards, blood alcohol testing and checking compliance with the obligations of officers and staff arising from their foreign business trips and receptions.

Except for minor cases, no infringements of generally binding legal regulations were found during the controls.

INTERNAL AUDIT

In 2022, 4 planned internal audits were carried out by the Internal Audit Unit to verify and assess.

- Compliance with art. 8f of Act No 278/1993 Coll. on the Management of State Property for the years 2020 and 2021 in the liable person of the NSA,
- economy, efficiency, effectiveness and expediency in managing public finances for the year 2021 in the liable person of the NSA,
- compliance with Act No 10/1996 Coll. on control in the state administration for the years 2020 and 2021 in the liable person of the NSA ,
- economy, efficiency, effectiveness and expediency in the managing public finances for the year 2021 in the liable person of the Cyber Security Competence and Certification Centre.

The performed internal audits identified 10 deficiencies of low and medium severity, which did not have financial consequences.

In accordance with Act No.357/2015 Coll. on financial control and audit, deadlines were set for the liable persons to take measures to remedy the deficiencies and to eliminate the causes of their occurrence, to send a list of the measures taken and to comply with the measures taken.

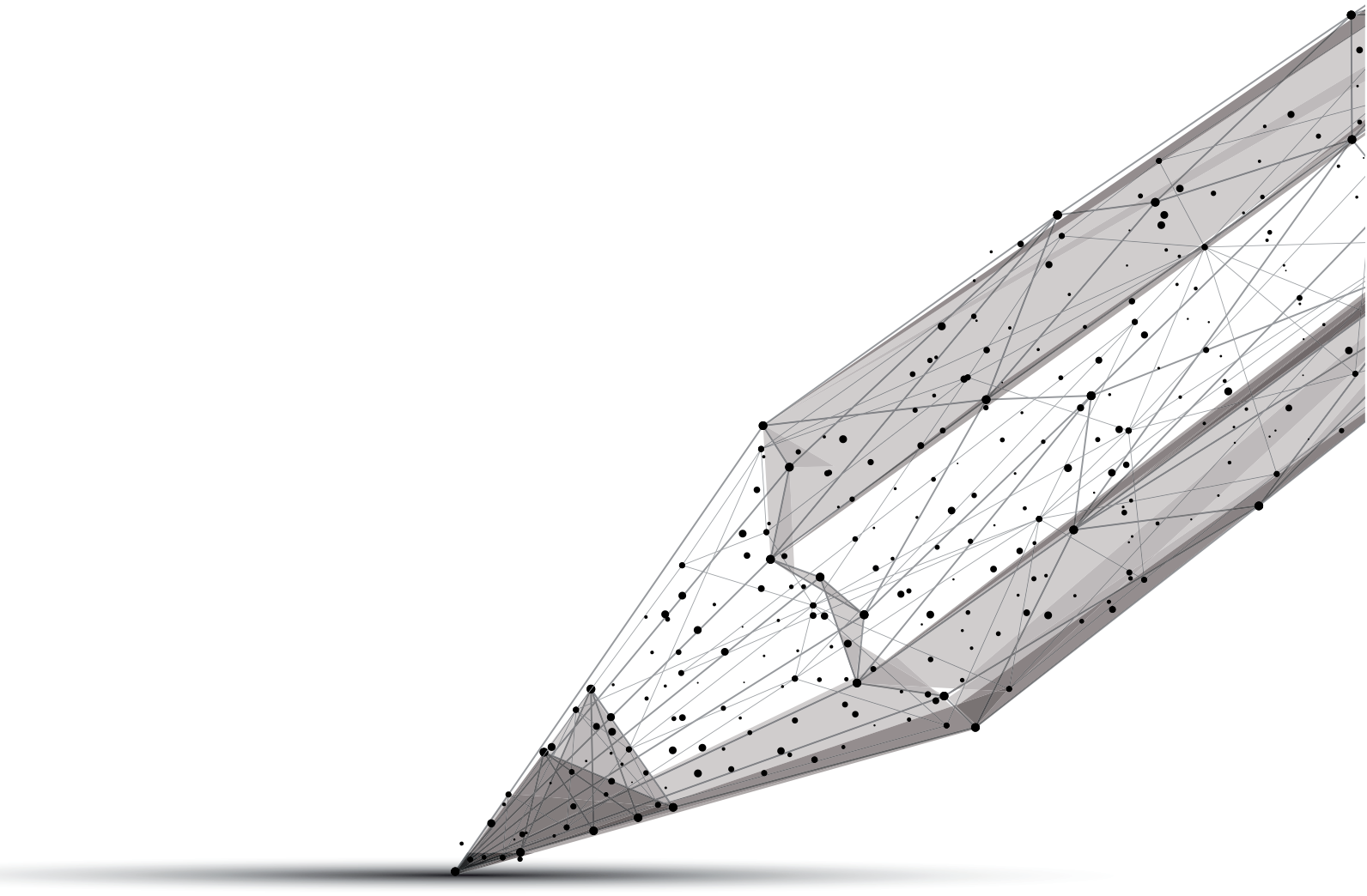
SECURITY RISKS

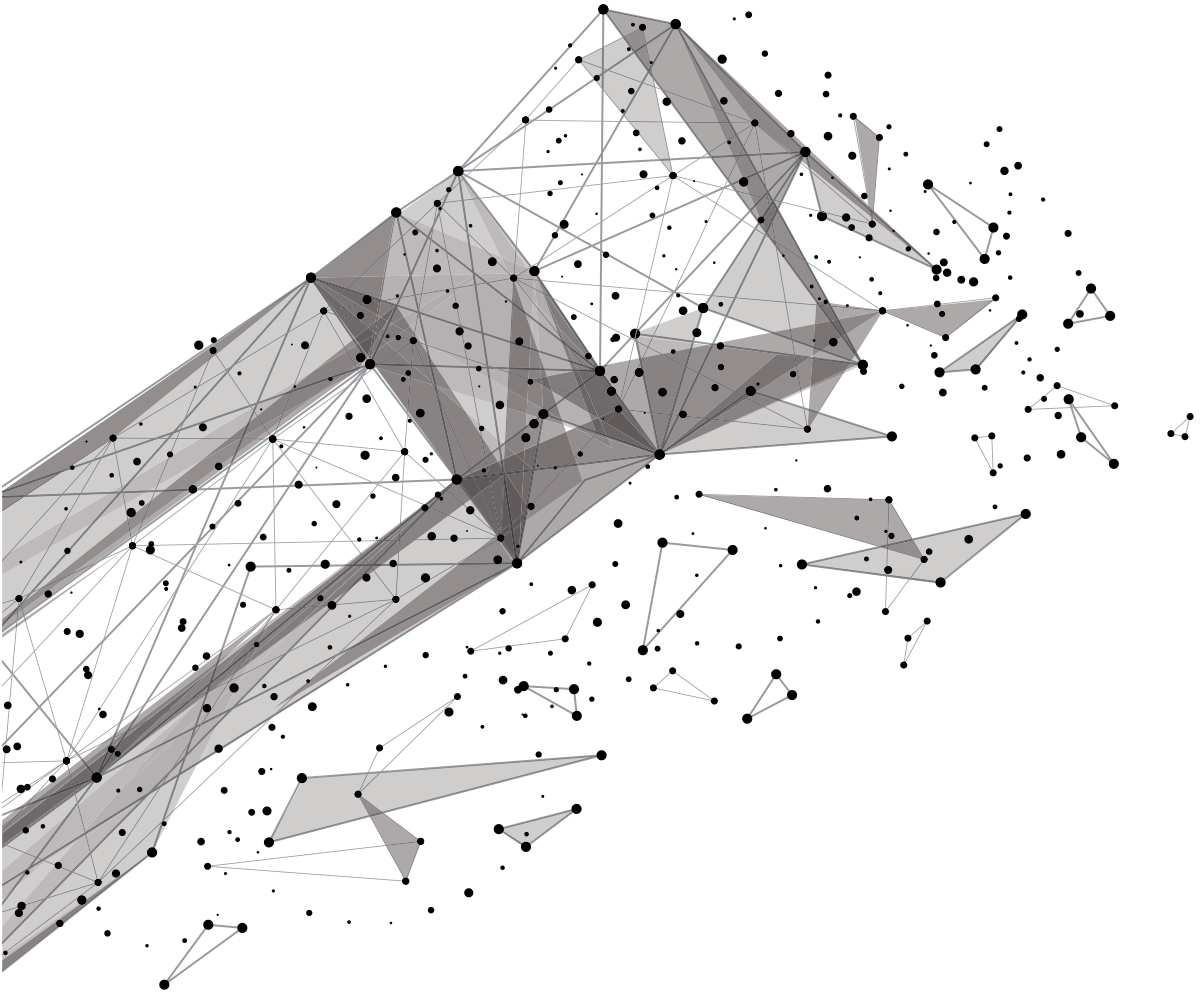
In 2022, the NSA collected, concentrated, analyzed, and reviewed information on security risks in the area of internal security related to the scope of the NSA, its officers, and employees.

COMPLAINTS AND PETITIONS

The NSA received 3 complaints which the NSA assessed as unfounded by investigation/ review and 1 submission marked as a complaint, which, however, according to the content, was not a complaint within the meaning of Act No 9/2010 Coll. on complaints. No petition was received by the Authority in 2022.

PRIORITIES FOR 2023





In the area of trust services, the National Security Authority will upgrade selected operational components of the trust infrastructure.

In the area of cryptographic protection of information, the NSA will continue to build a secure infrastructure in individual segments.

The education and training of specialists at professional courses, seminars and trainings at home and abroad in order to acquire new skills and deepen their qualification remains a priority.

The NSA will continuously develop capabilities in the area of certification of mechanical prevention devices, technical safeguarding devices and technical means or cryptographic protection devices.

Priorities for 2023 also include implementation of projects:

- Electronic Services for Processing Security Files of the National Security Authority project, which is aimed at creating information systems for the electronisation of the NSA's services in the field of protection of classified information and internal processes related to security clearances of natural persons and entrepreneurs,
- project to build new physical and building security,
- CAF (Common Assessment Framework) model implementation project aimed at the development of the management system and the international quality certificate.