KEY TRENDS AND STATISTICS OF THE NATIONAL CYBER SECURITY STATUS OF LITHUANIA

2022

MINISTRY OF NATIONAL DEFENCE
REPUBLIC OF LITHUANIA

NCC
CYBERSECURITY NATIONAL
COORDINATION CENTRE
LITHUANIA

KEY TRENDS AND STATISTICS OF THE NATIONAL CYBER SECURITY STATUS OF LITHUANIA

2022

MINISTRY OF NATIONAL DEFENCE
REPUBLIC OF LITHUANIA

NCC
CYBERSECURITY NATIONAL
COORDINATION CENTRE
LITHUANIA

Cyber security threats, hostile state interests and the impact of societal resilience on national cyber security status of Lithuania

1. In 2022, enhancement of the supply chain security of Lithuanian contracting authorities was continued, Lithuania proceeded with the preparation of the National Cyber Security Development Programme, and adopted a description of the procedures regulating the availability and recovery of state information resources

In 2022, Lithuania adopted legislation to ensure that only equipment from trusted manufacturers is used in critical infrastructure, including 5G infrastructure. Amendments to the Law on Public Procurement[01], the Law on the Procurement by Contracting Authorities Operating in the Water, Energy, Transport and Postal Services Sectors[02], and the Law on Procurement in the Field of Defence and Security[03] of the Republic of Lithuania were adopted in order to manage the risks to national security arising from the use of unreliable information technology in critical state infrastructure.

During the course of 2022 the preparation of the National Cyber Security Development Programme (hereinafter, the Programme) initiated in 2021 continued, consistently involving various state institutions in its implementation. Part of the activities of the Programme will be funded by the 'New Generation Lithuania' funds within the framework of the Recovery and Resilience Facility, allocating EUR 40.15 million in total.

The Ministry of National Defence of the Republic of Lithuania (hereinafter, the MoND) was a party in drawing up the Description of the procedure for storing copies of state information resources which have to be made available in cases of martial law, state of emergency, emergency situations or other crises in data centres in the Member States of the European Union, the Member States of the European Economic Area (EEA) and/or the Member States of the North Atlantic Treaty Organisation (NATO), and for the procedure for restoring the functioning of these resources from copies. This procedure description was approved by the Government by its Resolution No. 739[04] of 11 July 2022. It determines the actions of the institution authorised by the Government of the Republic of Lithuania and the managers of the registers and state information systems included in the list approved by the Government Resolution, as well as the managers of these systems. The procedure allows to ensure that state information resources are accessible in the event of a state of war, a state of emergency, or in case of any other crises, and to thus guarantee their protection.

2. International cooperation in the field of cyber security defence remains one of Lithuania's priorities in strengthening national and regional capabilities

On 7 November 2022, the MoND, together with representatives of the Czech Presidency of the Council of the European Union and the European Union Agency for Cybersecurity (hereinafter, the ENISA) hosted in Lithuania the annual crisis management exercise BlueOLEX 2022, which is intended to further contribute to the EU operational (European Liaison Cyber Crisis Liaison Organisation Network's (CyCLONe)) level common coordination in case of a large-scale cyber incident/crisis. The participants of the 2022 exercise in Vilnius included representatives from 22 EU Member States, as well as from the European Commission and the ENISA.

The National Coordination Centre (NCC) became operational in 2022.The MoND carries out its tasks in accordance with Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre[05] (hereinafter, the ECCC) and the Network of National Coordination Centres.

[01] The Law on the Amendment of Articles 2, 17, 25, 27, 35, 37, 39, 45, 47, 51, 90 and 92 of the Law on Public Procurement No. I-1491 of the Republic of Lithuania, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/0ed02bd3a5ff11ecaf79c2120caf5094?positionInSearchResults=1&searchMoNDelUUID=90d1a3c6-7c67-4c0e-8293-f08f9cb05fd0.

[02] Law on the Amendment of Articles 2, 29, 37, 39, 48, 50, 52, 58, 98 and 100 of the Law on the Procurement by Contracting Authorities Operating in the Water, Energy, Transport and Postal Services Sectors No. XIII-328 of the Republic of Lithuania, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/409b3602a5ff11ecaf79c2120caf5094?positionInSearchResults=0&searchMoNDelUUID=c763dc84-b132-4afa-ac32-baad3018a0f2.

[03] Law on the Amendment of Public Procurement in the Field of Defense and Security (https://eseimas.lrs.lt/portal/legalAct/lt/TAD/83c76892a5ff11ecaf79c2120caf5094) aimed at effectively managing risks arising to national security due to insecure (unreliable) information technologies in critical state infrastructure.

[04] Description of the procedure for storing copies of State information resources to be made available in cases of martial law, state of emergency, emergency situations or other crises in data centres in the Member States of the European Union, the Member States of the European Economic Area (EEA) and/or the Member States of the North Atlantic Treaty Organisation (NATO), and for the procedure for restoring the functioning of these resources from copies, https://e- seimas.lrs.lt/portal/legalAct/lt/TAD/77 9cbbc401a711edbfe9c72e552dd5bd?positionInSearchResults=6&searchMo delUUID=0a605674-93d7-4635-“acf9- 7c35ea7543a7.

[05] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021, https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32021R0887&from=EN.

The Lithuanian NCC, being a part of this European network, is supported by partners: the National Cyber Security Centre under the Ministry of National Defence (NCSC), Innovation Agency and Central Project Management Agency (CPMA). With funding from the Digital Europe Programme and the state budget of the Republic of Lithuania, the NCC will launch calls for funding of up to EUR 60,000 for small and medium-sized enterprises (SMEs) projects in the field of cyber security innovations (e.g. Cyber security solutions in the field of EdTech and cyber security solutions for resilience building in SMEs). The Lithuanian NCC will also carry out other activities that are typical for NCCs across the EU, such as promotion of cyber security culture, building and informing the Lithuanian cyber security community, promotion and dissemination of cyber security education programmes, and sharing of expert knowledge in the area of cyber security.

In 2022, development of the Regional Cyber Defence Centre (RCDC), which operates as a branch of the NCSC, continued. The RCDC has produced and shared with partners more than 40 cyber threat intelligence reports and cyber incident analyses. The documents provided a clearer understanding of the most pressing cyber incidents in the region.

A training programme for cadets of the Ukrainian Armed Forces was also developed and a pilot course was completed. The internship programme for Ukrainian cadets at the RCDC, launched in 2023, will allow them to gain valuable practical knowledge and to use it in the service, being also one of Lithuania's means of support to Ukraine.

In May 2022 the NCSC signed a Memorandum of Understanding with the Polish National Cyber Security Centre - Cyber Security Headquarters. In autumn 2022, decision of Poland's accession to the RCDC was taken and in January 2023 the necessary agreements allowing Poland to become a member of the RCDC were signed. In addition, in 2022 a joint Lithuanian-Polish team won second place (out of 24) in the world's largest cyber-defence exercise, Locked Shields 2022.

In the spring of 2022, experts from the NCSC in cooperation with representatives of the USA Cyber Command successfully executed operation Hunt Forward, with the main objective to strengthen practical interoperability and increase the resilience of critical networks to cyber threats. Between 2021 and 2022, Lithuania also participated in the Counter Ransomware Initiative, a US-led international initiative to unite 36 countries in fight against ransomware attacks orchestrated by Russia and other countries, to strengthen the resilience of networks, and to disrupt the infrastructure of criminal groups.

3. Against the backdrop of Russia's invasion of Ukraine, the EU has taken action to assist Ukraine and secure its cyberspace in the face of increased cyber security threats

Cyber attacks have been an integral part of Russia's military aggression against Ukraine since the beginning of 2022. The attacks affected not only Ukraine, but also other EU and NATO countries. The EU's cyber agenda for 2022 was mainly focused on providing full support to Ukraine from the EU and EU Member States and coordinating EU legislative proposals in the field of cyber security. In 2022, Lithuania, together with other EU Member States, actively provided cyber security support to Ukraine, also supplying it with the necessary equipment and software.

On 22 February 2022 Lithuania, the Netherlands, Poland, Estonia, Romania and Croatia activated the EU Cyber Rapid Response Teams (CRRTs)[06] in response to the request of 18 February 2022 for cyber support made by the Minister of Foreign Affairs of Ukraine, Mr Dmytro Kuleba, to the representatives of the EU Institutions and Member States. In November 2022, the EU Cyber Rapid Response Teams provided support to Moldova and conducted a vulnerability assessment[07].

On 10 May 2022, the EU has officially attributed the attack to Russia for the first time, as it carried out a cyber attack on the KA-SAT satellite network operated by US satellite operator Viasat just hours before the massive invasion of Ukraine. The attack disrupted internet services not only in Ukraine, but also in Germany, France, Hungary, Greece, Italy, Hungary and Poland. On 19 July 2022, on Lithuania's initiative, a joint EU declaration was issued on the pro-Russian cyber hacking attacks against Lithuania and other European countries in the context of the Russian war in Ukraine.

In order to deter cyber threats and attacks against the EU and EU Member States from third countries or criminal actors, the Council of the EU in May 2022 extended the duration of the cyber-restrictive measures' framework for three years, until 2025. Under this framework, the EU can impose tailored restrictive measures on individuals or entities linked to cyber attacks that have a significant impact and pose an external threat to the EU or its Member States. The cyber sanctions list currently includes eight individuals and four entities from Russia, China and North Korea.

4. In 2022, EU legislative initiatives in the field of cyber security were mainly focused on increasing the overall high level of cyber security and the security of hardware and software products

After two years of negotiations, 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, (NIS2) (hereafter, the NIS2) , which will reinforce the resilience of cyber resilience and the capacity of the public, the private sector and the EU as a whole, was published in the Official Journal of the European Union (EU Official Journal)[08]. NIS2 entered into force on 16 January 2023, allowing Member States 21 months to transpose the provisions of this EU law.

On 15 September 2022, the European Commission presented a new proposal for an EU Regulation on the Cyber Resilience Act (CRA). The aim of the legislation is to establish horizontal mandatory cyber security requirements for hardware and software products throughout their entire life cycle. Lithuania, like other EU countries, agrees that only technologies that meet the highest standards of resilience, protection and security should be allowed to enter the EU market. The ongoing EU Council negotiations are refining the provisions of the legislative proposal.

5. In 2022, the NCSC's Incident Response Team (CERT-LT) recorded a total of 4,080 cyber incidents, a number similar to that of 2021. In contrast to previous years, the number of Distributed Denial of Services (DDoS) attacks increased

CERT-LT recorded a total of 4,080 cyber incidents in 2022, which is by 8 incidents less than in 2021. Of the total number of incidents recorded in 2022, 33 are in the medium category and are related to DDoS attacks and the distribution of malicious code to gain access to communication information systems to carry out malicious activities (e.g. espionage, destructive actions, etc.). Compared to 2021, the number of medium category incidents in 2022 has decreased by 35 per cent (2021 -- 93 incidents).

[06] The Cyber Rapid Response Teams operates under the EU's Permanent Structured Cooperation (PESCO) project led by Lithuania.

[07] In March 2023, the Cyber Rapid Response Teams supported the EU military mission in Mozambique and conducted a vulnerability assessment.

[08] NIS2, https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=lt.

Looking at all cyber incidents recorded by the NCSC in 2022, as in the previous year, the majority of incidents were related to the proliferation of malicious software (phishing, distribution of unwanted information, hacking attempts). However, in contrast to previous years, the number of DDoS attacks increased.

At the end of June 2022, the NCSC recorded a huge wave of DDoS attacks against the public and private sectors. From gathered public information sources the attempts were aimed at 130 publicly accessible websites. A pro-Russian Federation hacker group claimed responsibility for the attacks. The attacks did not damage the companies' information systems, and even had a positive effect, as information system administrators and managers started to prioritise and additionally finance their cyber security to enhance it.

Likewise, similar trends are observable in Europe. According to ENISA's annual threat review[09], in terms of frequency and impact, on the second place is malware, and on the third place is social engineering with phishing remained as a most popular technique. According to ENISA, ransomware attacks stands on the first place and 60 per cent of affected organisations may have paid ransom demands.

In Lithuania, the largest number of cyber incidents in 2022, as in previous years, was recorded in the infrastructures of hosting service providers that can be used to create websites, virtual workstations, provide e-mail services, etc. Such numerous incidents was due to two reasons: vulnerable websites and the possibility to purchase hosting services anonymously in Lithuania by paying for services in cryptocurrency, which creates anonymity for buyers and makes their traceability difficult, if at all possible.

6. The impact of the war on Ukraine's cyber security environment

Since 2014 Russia's cyber-attacks against Ukraine and particularly just right before the war have intensified. On 13-14 January 2022, more than 70 websites of Ukrainian government institutions were defaced spreading disinformation in Russian, Ukrainian and Polish. The attacks continued in February, with two massive cyberattacks just a few days before the start of military invasion. On 16 February 2023, a DDos attack was carried out against hundreds of Ukrainian websites, followed by an attack of wiper malware against hundreds of Ukrainian state information systems, as well as the country's energy, information technology, media and financial sectors. The main purpose of these attacks was to undermine the confidence of the population in the Ukrainian state and leaders and to weaken the will of the population to resist.

According to the Ukrainian cyber incident management team CERT-UA, a total of 2,245 incidents were recorded between the beginning of the mass invasion of Ukraine on 24 February 2022 and 1 February 2023: cases of use of malicious software engineering (SE) (568), phishing (552) and successful hacking (394). The largest number of cyber incidents was recorded in the infrastructure of organizations operating in the state and municipal spheres (564), in the field of security and defence (312), as well as business (159).

The war also influenced the activities of hacktivist groups, which joined both sides and actively began to support them. Pro-Ukraine cyber activist groups, such as the Ukrainian IT Army, claimed to have hacked into Russia's most important authorities and gained access to a huge amount of important information, disrupted the activities of major media outlets and carried out other harmful actions. On the other side, the pro-Russian activist group was mainly announcing wider-scale or smaller DDoS attacks in both Europe and the U.S.

Cyberattacks on Ukraine's critical infrastructure were carried out throughout 2022. At the beginning of the war, cyber-attacks were more complex, they were prepared in advance, sometimes even up to 6 months. Latter the attacks were simpler, such as DDoS, attempts to extort sensitive data based on the principles of social engineering, spreading disinformation, etc.

7. In response to the events in Ukraine and changes in cyber security environment, the NCSC actively provided recommendations to critical infrastructure managers on preventive cyber security measures, with a particular focus on business continuity plans and training

In 2022, the assessment of the capacity of national institutions to use the Secure State Data Transmission Network in the case of internet blackout was organized.[10] In order to ensure the safe and fast exchange of information on possible threats between cyber security entities and the NCSC, a closed chat platform and data exchange module were developed in the Cyber Security Information Network (hereinafter, the CSIN).

State and critical information infrastructure staff were also encouraged to responsibly assess increased cyber security risks. Training was considered a very high priority by the NCSC, with more than 1,200 state and municipal employees completing complex three-day cyber security training, and 2,400 civil servants have undergone NCSC shorter training on various basic cyber security knowledge topics. A special course was also organized for Lithuanian non-governmental organizations working on support for Ukraine.

In cooperation with Kaunas University of Technology (hereinafter, the KTU) the NCSC organized the largest national cybersecurity exercise Cyber Shield 2022 in terms of the number of participants. The representatives from 116 organizations, including 107 managers of state information resources and managers of critical information resources, tested their processes and procedures in managing cyber incidents. Phishing awareness training was conducted by using a social engineering tool goPhish. It sent users mock phishing emails that were designed to look genuine. About 13 per cent of all receivers did not recognized mock emails and performed some harmful actions. This demonstrates the need for continuous education of employees.

In 2022 the NCSC started operating cyber range and more than 160 persons from Lithuania and 58 foreign partners tested their profession skills in this training infrastructure. The NCSC's cyber range was also used in the national cyber security exercise Cyber Shield 2022. This opportunity was used by 92 participants from 25 organisations.

In 2022, the NCSC acted as the national coordinator for Lithuanian participation in the largest EU cyber security exercise Cyber Europe 2022. The 8 largest national health care institutions, as well as CERT-LT, the Ministry of Health and the Centre of Registers participated in this exercise. To combat lightning-fast phishing attacks, the NCSC, together with KTU Internet Service Centre DOMREG, developed and launched a new free tool for residents and organizations – a DNS firewall. By the end of the year, the DNS firewall was voluntarily installed not only by residents and business organizations, but also by part of the critical information infrastructure managers.

[09] ENISA Threat Landscape 2022, ENISA, https://www.enisa.europa. eu/publications/ enisa-threat- landscape-2022.

[10] The organizer of the exercise is the Core Center of State Telecommunications.

8. The NCSC carried out inspections of critical information resources, cyber threat assessments in the networks of cyber security entities

In 2022, the NCSC launched a cyber threat search in the networks of cybersecurity entities. During the first year of this activity, 184 potential threats were identified, the entities were informed about such threats either directly or through internet service providers.

The NCSC continued coordinating responsible disclosure activities, and during 2022, the NCSC received 51 reports from cyber security professionals about possible loopholes on the websites of state institutions. Valuable information was obtained about the security gaps in important systems; among such systems were the document management system 'Avilys' which is popular in the public sector and information systems managed by the public sector. In 2021, in line with the principles of responsible disclosure, the NCSC received 81 reports of various faults in cyber security.

The NCSC conducted critical information resource inspections to determine the compliance of critical information resource managers with organisational and technical cyber security requirements (hereinafter, the OTR). Over the year total six inspections were carried out (1 of them repeatedly) in the energy, transport, civil protection and water supply sectors (5 inspections were carried out in 2021).

During the year, the NCSC assessed 279 state information resource security documents, of which 199 were approved, some comments were issued regarding the others. In order to check the compliance of the state's information resource manager with the requirements of security documents, one pilot inspection of the state's information resource manager was carried out in 2022. The NCSC seeks to be authorised to carry out regular inspections of the state's information resources.

9. According to the Communications Regulatory Authority (hereinafter, the RRT), the capacity of the public communications networks has been and is sufficient, and the networks continue to be responsibly planned, monitored and evaluated

In 2022, the RRT received 7 reports (8 reports in 2021) from three providers on the breach of the integrity of public communications networks. Despite one larger-scale breach of the integrity of public communications networks, the capacity of public communications networks has been and is sufficient, the networks are being planned and monitored with due responsibility. Such a conclusion is drawn from the reports submitted by the providers to the RRT about violations of the integrity of the public communications networks, additional information received every three months and the additional assessment of the indicators for measuring the quality of public electronic communications services by the RRT during continuous monitoring.

In 2022, no more network faults were recorded in the public mobile and public fixed communications networks than in previous years. Identified faults were eliminated promptly and the extent of violations of the integrity of public communication networks did not lead to extreme events that would have required additional actions and/or informing of other institutions in accordance with the procedure established by legal acts.

In 2022, through its hotline the RRT received 1,523 reports of potentially prohibited information or content negatively affecting minors observed on the Internet; 694 of the reports (253 repetitive) were confirmed, and 441 cases were followed up (representing 29 per cent of all notifications received). Compared to 2021, when 3,558 notifications were received, there is a downward trend. It is important to mention that the number of messages received on the RRT Internet hotline is constantly changing.

In 2022, fewer reports of images of child sexual exploitation were received in the Lithuanian internet space due to the fact that the Lithuanian information hosting service provider through whose servers the child sexual exploitation material was actively publicized was identified in 2021, and the information was removed. The RRT hotline is used to report on any violations by both responsible citizens and members of the INHOPE network of the international association of internet hotlines and provides extremely accurate and reliable data.

In previous years, the success of the RRT's fight against content on the Internet that is prohibited and has a negative impact on minors is due to the fact that internet users were reporting content related to pornography, child sexual exploitation, violence, etc. via the RRT's Clean Internet hotline. Since the beginning of 2022, RRT, in order to make the process of detecting prohibited information more efficient, uses an innovative, artificial intelligence-based solution developed in cooperation with the Oxylabs company. This automatic search tool searches for prohibited Internet content in the Lithuanian IP address space and informs the RRT Clean Internet hotline

10. According to the data of the Lithuanian Police, in 2022 the increase in crime registered in Lithuania was mainly due to the increase of criminal activities in cyberspace

In 2022, the country's police authorities recorded 42,988 criminal offences, of which 5,309 offences, or 12 per cent, were committed in cyberspace. In 2022, compared to 2021, the number of cyber crimes increased by 2,775 cases, or 52 per cent.

As in the last few years, the most common types of cyber crimes was fraud (Article 182 of the Criminal Code of the Republic of Lithuania), and in 2022 accounted for the majority – 48 per cent – of all criminal offences committed in cyberspace. The structure of the dominant methods of fraud has not changed and advance (prepayment) fraud has remained a prevailing type of fraud.

According to the data of the Lithuanian Banking Association (hereinafter, the LBA), financial fraudsters extorted almost EUR 12 million from Lithuanian residents and companies in 2022[11]. During the same period, through the efforts of financial institutions and law enforcement, about EUR 5 million was returned to the owners. Although the amount of fraudulently extorted funds increased relatively marginally (in 2021, EUR 10.2 million were extorted), the number of recorded incidents more than doubled. In 2022, compared to 2021, the number of incidents has increased from 3,500 to nearly 8,000. These statistical indicators show not only the growing activity of fraudsters, but also the greater openness of the public on this topic – victims are more open in telling about their experiences, more actively reporting to banks about the fraud they have experienced, or any threatening fraud, thereby contributing to the faster prevention of crime.

According to the data of the Lithuanian police, in 2022, the largest damage of EUR 457,142 was suffered by an insurance company in Vilnius when a fraudulent bank account has intruded into electronic communication.

[11] LBA data, https://www.lba.lt/lt/apie- mus/ asociacijos-naujienos/finansiniai- sukciai-pernai-isviliojo-12-mln-euru- savininkams-grazinti-5-mln-euru.

According to the data of the Department of Informatics and Communications under the Ministry of the Interior of the Republic of Lithuania (hereinafter, the IRD under the MoI of the Republic of Lithuania), 919 security crimes of electronic data and information systems were registered in the country in 2022. These crimes are referred to in Articles 196-198(2) of the Criminal Code of the RL, and accounted for 2 per cent of the total recorded crimes. In 2021, 707 such crimes were recorded (down by 212 (30 per cent)).

There is an increasingly evident trend for persons committing criminal acts in Lithuania to act not individually, but in well-organized groups. It is difficult to investigate such groups and criminal acts of this kind due to the abundance of technologies, legal difficulties associated both with determining the place where such acts were committed and with obtaining data (information) relevant for the pre-trial investigation from third parties. Not only Lithuanian, but also foreign natural and legal persons suffer from these criminal acts.

11. The number of recorded personal data breaches (hereinafter, the PDB) received by the State Data Protection Inspectorate (hereinafter, the SDPI) is systematically increasing, however, this is not related to the increase in the number of violations themselves, but rather to an increase in the knowledge gained by data controllers and awareness in the field of personal data protection

The number of reports on PDB received by the SDPI is increasing every year (100 in 2018, 175 in 2019, 181 in 2020, 239 in 2021 and 304 in 2022). The SDPI notes that in 2022, as before, most PDBs consisted of phishing and ransomware attacks. The data controllers suffered quite serious damage because of these attacks and had to devote significant financial and human resources to managing these PDB and reducing their impact. Other personal data security vulnerabilities were related to social engineering and data grooming techniques, supply chain attacks, gaps in access control management organizations' computer networks.

According to the nature of PDB, confidentiality violations are statistically prevalent in Lithuania, their number is consistently growing every year - in 2022, the confidentiality of personal data was lost in as many as 269 cases (out of all 304 registered).

Russia's war in Ukraine caused an even greater wave of cyber attacks and worsened the cyber security situation in the world. Although the SDPI did not develop special measures in the context of the Russian war due to the increased threat to the personal data processed by organizations, the SDPI in its contacts with data controllers and processors emphasized the need to pay even more attention to appropriate technical and organizational measures for the processing of personal data.

12. In the context of information confrontation the year 2022 was exceptional

In 2022, the total number of cases of information activities hostile to Lithuania amounted to 4,999 unique information cases.

Compared to the data of the last five years, the number of information incidents in 2022 has remained quite high, although the number of information cases has decreased compared to 2021. The escalation of defence topics almost doubled in 2022: In 2021, the defence-related instances accounted for 26.42 per cent of all unique cases, and in 2022 - 47.91 per cent. This coincided with significant foreign and domestic events, which unfriendly sources of information sought to use in order to create a negative image of Lithuania in the West and to promote the confrontation between the audiences of Lithuanian society. The Kremlin and Belarus regime-controlled information sources specifically focused on the following defence related topics: NATO, NATO for capacity building in the Baltic region, Lithuania's NATO membership, strengthening Lithuania's military potential. Significant attention was dedicated to Lithuania's foreign policy, i.e., bilateral and multilateral relations, membership in international organizations, support for Ukraine.

In 2022, the abundance of political and security-enhancing processes in which the Republic of Lithuania actively participated or were directly related to also led to a greater negative attention of Russia and Belarus to Lithuania. Hostile information activities related to three strategic areas: (1) defence; (2) foreign policy; and (3) protection of constitutional foundations.

In 2022, the narrative related to defence focused on disinformation about NATO as an institution, NATO-Russia relations. Russia's aggressive propaganda tone about NATO as a provocateur and the culprit of the allegedly deteriorating global security situation, which began in 2021, did not cease in 2022, directly blaming the U.S. and NATO for starting the war in Ukraine.

In 2022, the number of instances of hostile information operations against Lithuania and state institutions was lower than in 2021. The number of cases of information operations and cyber attacks against Lithuanian institutions decreased as most of such attacks targeted Ukrainian state institutions.

Issued by the Ministry of National Defence of the Republic of Lithuania,
Totorių g. 25, LT-01121 Vilnius, www.kam.lt
01/06/2023. Order No GL-268

Layout by the Visual Information Division of the General Affairs Department
of the Ministry of National Defence, Totorių g. 25, LT-01121 Vilnius
Printed by the Military Cartography Centre of the Lithuanian Armed Forces,
Muitinės g. 4, Domeikava, LT-54359 Kaunas district

Illustrations from the Freepik.com graphic recource platform were used

KEY TRENDS AND STATISTICS OF THE NATIONAL CYBER SECURITY STATUS OF LITHUANIA

2022