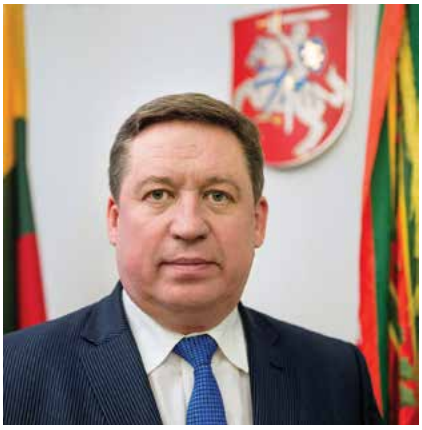
MINISTRY OF NATIONAL DEFENCE
REPUBLIC OF LITHUANIA

NATIONAL CYBER SECURITY STRATEGY

NATIONAL CYBER SECURITY STRATEGY

APPROVED
by Resolution No. 818 of the Government
of the Republic of Lithuania of 13 August 2018

CONTENTS



It is evident that information and communication technology has changed and is still changing our lives at a rapid pace thus having a great impact on the activities of private and public sectors. Undoubtedly, any damage to a state's critical infrastructure through the use of malicious software in combination with a disinformation campaign might lead to chaos in a country. The number of cyber incidents grows by 10% every year; the incidents become increasingly complex: cyber-attacks last longer and are better coordinated. For this reason, current threats must be countered in an expedient manner using new measures and tools.

The Ministry of National Defence has prepared the National Cyber Security Strategy which demonstrates one more step forward made towards ensuring cyber security of the country. The Strategy is a key document which sets the aims and objectives of Lithuania's public and private sectors as well as research and educational institutions for the next five years. The Strategy takes a holistic approach, where cyber security is seen as an integral part of digital ecosystem rather than an independent national goal or as a set of tools designed for responding to challenges of the digital age.

Our aim is to raise public awareness and enhance the resistance of the Lithuanian society to cyber incidents which pose national security threats, present risks to the fulfilment of functions assigned to the governmental and municipal authorities and institutions as well as to the provision of e. public services rendered by such public bodies, to the development of business, to personal data protection and to the fundamental rights and freedoms of individuals. I am confident that we will considerably strengthen Lithuania's cyber resistance, if we respond to the most relevant challenges the Lithuanian digital society and economy faces and take the responsibility for the security of our activities in cyber space all together.

R. Karoblis r

Raimundas Karoblis,
Minister of National Defence

The main purpose of the Strategy is to provide the Lithuanian people with the opportunity to explore the potential of information and communications technology (ICT) by identifying cyber incidents timely and effectively, by preventing cyber incidents and their recurrence, and by managing the impact of cybersecurity breaches.

- **THE FIRST** target of the Strategy –
to strengthen cyber security of the country and the development
of cyber defence capabilities.

- **THE SECOND** target of the Strategy –
to ensure prevention and
investigation of criminal offences in cyber space.

- **THE THIRD** target of the Strategy –
to promote cyber security culture and development of innovation.

- **THE FOURTH** target of the Strategy –
to strengthen a close cooperation between private and public sectors.

- **THE FIFTH** target of the Strategy –
to enhance international cooperation and ensure
the fulfilment of international obligations in the field of cyber security.

1

General Provisions

1. The National Cyber Security Strategy (hereinafter referred to as the "Strategy") defines the most important pillars of the national cyber security policy. The Strategy is aimed at strengthening the development of the state's cyber security and cyber defence capabilities preventing and investigating cybercrimes, promoting cyber security culture and the development of innovation, enhancing close private-public partnership (PPP) and international cooperation, and ensuring the fulfilment of international cyber security obligations within the country until 2023.

2. The Strategy has been developed in consideration of the environmental analysis, data from the conducted research, and suggestions offered by public and private sector representatives. It meets the provisions of the Programme of the Seventeenth Government of the Republic of Lithuania, which was accepted by Resolution No. XIII-82 of the Seimas of the Republic of Lithuania of 13 December 2016 "On the Programme of the Government of the Republic of Lithuania" (hereinafter referred to as the "Programme of the Government of the Republic of Lithuania"), the National Security Strategy approved by Resolution No. IX-907 of the Seimas of the Republic of Lithuania of 28 May 2002 "On the Approval of the National Security Strategy", the Law of the Republic of Lithuania on Cyber Security, the communications and recommendations made by the European Parliament, the Council, and the European Commission in the field of cyber security as well as the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A Digital Single Market Strategy for Europe" dated 6 May 2015 and the Lithuanian Information Society Development Programme 2014–2020 "Digital Agenda of the Republic of Lithuania" approved by Resolution No. 244 of the Government of the Republic of Lithuania of 12 March 2014 "On the Approval of Lithuanian Information Society Development Programme 2014-2020 "Digital Agenda of the Republic of Lithuania". After Lithuania joined the Organisation for Economic Co-operation and Development (OECD), recommendations produced by this organisation on Digital Security Risk Management for Economic and Social Prosperity have also become part of the key guidelines reflected in the Strategy.

3. Terms used in the Strategy shall have the same meanings as those defined in the Law on Cyber Security, the Law of the Republic of Lithuania on the Organisation of the National Defence System and Military Service, the Law of the Republic of Lithuania on Higher Education and Research and the Law of the Republic of Lithuania on the Right to Obtain Information from State and Municipal Institutions and Agencies.

© iStock

2

Targets and Objectives of the Strategy, evaluation criteria and their Values

Cyber Security and Cyber Defence Capabilities of the State

5. **The first target of the Strategy is** to strengthen cyber security in the country and to develop cyber defence capabilities.

6. Like other countries of the world that have well-developed broadband infrastructures and in which ICT potential is being actively explored, Lithuania has become attractive not only to individuals, groups of individuals or organised groups but also to the countries specified in the reports of national security threats and issued annually by the State Security Department of the Republic of Lithuania and the Second Investigation Department under the Ministry of National Defence of the Republic of Lithuania (hereinafter referred to as the "SSD" and "SID", accordingly). Those countries threaten Lithuania's national security and conduct hostile activities in global and Lithuanian cyberspace. Data collected by the National Cyber Security Centre under the Ministry of National Defence (NCSC), SSD and SID reveal that Lithuania continuously encounters various types of cyber incidents that are intended to encroach on the information resources and critical information infrastructures. According to forecasts, the number and extent of cyber incidents are expected to increase.[1]

7. According to data in the National Cyber Security Status Report 2017, the National Electronic Communication Networks and Information Security Incidents Investigation Unit (also referred to as the "Computer Emergency Response Team in Lithuania" or "CERT-LT") processed 54,414 cyber incidents in 2017. Also in 2017, the number of recorded cyber incidents was 10% higher than in 2016. While cyber-espionage attacks primarily target Lithuanian state information resources, private critical information infrastructures and other entities of strategic or significant importance to the national security are also at risk. While applying technical cyber security measures, the NCSC has identified that the highest number of malware was detected in the sectors of energy (27%), public security and legal order (22%) and foreign affairs and security policy (21%). Compared to 2016, malware has mostly spread in the fields of public security and legal order, foreign affairs and security policy and energy. The condition of public sector websites, which according to the National Cyber Security Status Report 2017 has deteriorated, also influence the state of cyber security.

8. The explosion of cyber incidents that is indicated in the annual reports of the NCSC, SSD and SID is proof that every cyber security entity must determine the amount of time, money and other resources to allot to the protection of their communication and information systems and provided services. Cyber security entities perform security risk assessments, but they are often of formal nature only and are conducted so as to comply with legal requirements or internationally recognised standards.

The *Risk Analysis Manual* published by the Ministry of the Interior of the Republic of Lithuania 12 years ago reflects the progress in risk assessment in the light of current conditions of research and innovation, but the security risk assessment methodology has changed over time and the understanding of risk assessment performance has transformed from the assurance of control environment to the holistic approach of risk assessment of organisations' activities.

9. Individual security risk assessment processes have already reached maturity level in Lithuania, however, on the national level, the security risk

[1] The State Security Department of the Republic of Lithuania and the Second Investigation Department under the Ministry of National Defence (2018). *National Security Threat Assessment;* National Cyber Security Centre under the Ministry of National Defence (2018). *National Cyber Security Status Report 2017.*

assessment culture and cyber security risk assessment processes are still fragmentary. Cyber security threats and security gaps have not been adequately analysed and holistically integrated into the process of risk assessment. Furthermore, rapid ICT development presents a challenge to ensuring that cyber security professionals have adequate knowledge, skills and practice.

10. In order to enhance the culture of effective cyber security policy making and implementation and to improve cyber security risk assessment and other requirements, the following changes occurred in 2018:

10.1. The provisions of the Law on Cyber Security were recast to improve organisation, management and control of the cyber security system; the competence, functions, rights and duties of state institutions responsible for cyber security policy making and implementation were specified; the duties and responsibilities of cyber security entities were defined in more detail, and additional cyber security assurance measures were established.

10.2. Regulatory functions of state information resources security, activities of public communications networks, public digital communication services and digital information hosting service providers were consolidated which enabled systematic cyberspace monitoring, and management of cyber incidents occurring in communication and information systems of cyber security entities. The NCSC is the only agency in Lithuania that organises cyber incident management and assists other state institutions, businesses and residents on the one stop shop principle.

11. Consolidation of capabilities aims at developing an integral cyber security management system in Lithuania to represent a systematic approach to the security management planning in any field, encouraging cyber security entities to focus on security management quality, reducing administrative burden falling on cyber security entities, ensuring systematic assessment and evidence-based security management culture, and facilitating optimisation of security expenditure planning. Consolidation of capabilities also aims at ensuring sustainable development of cyber security competences and enhancement of regional cyber security capabilities.

12. The Ministry of National Defence of the Republic of Lithuania and the NCSC continuously cooperate with cyber security entities, consult them on cyber security issues, and organise cyber security exercises.

In 2017, the national cyber security exercise *Cyber Security 2017* had around 200 participants from over 50 organisations of private and public sector. In cooperation with the Communications Regulatory Authority of the Republic of Lithuania, the Lithuanian Police and the State Data Protection Inspectorate, workshops for representatives of cyber security entities were organised. Participants were familiarised with the requirements of legal acts related to cyber security and had training on management and counteraction to cyber incidents against critical communication and information systems.

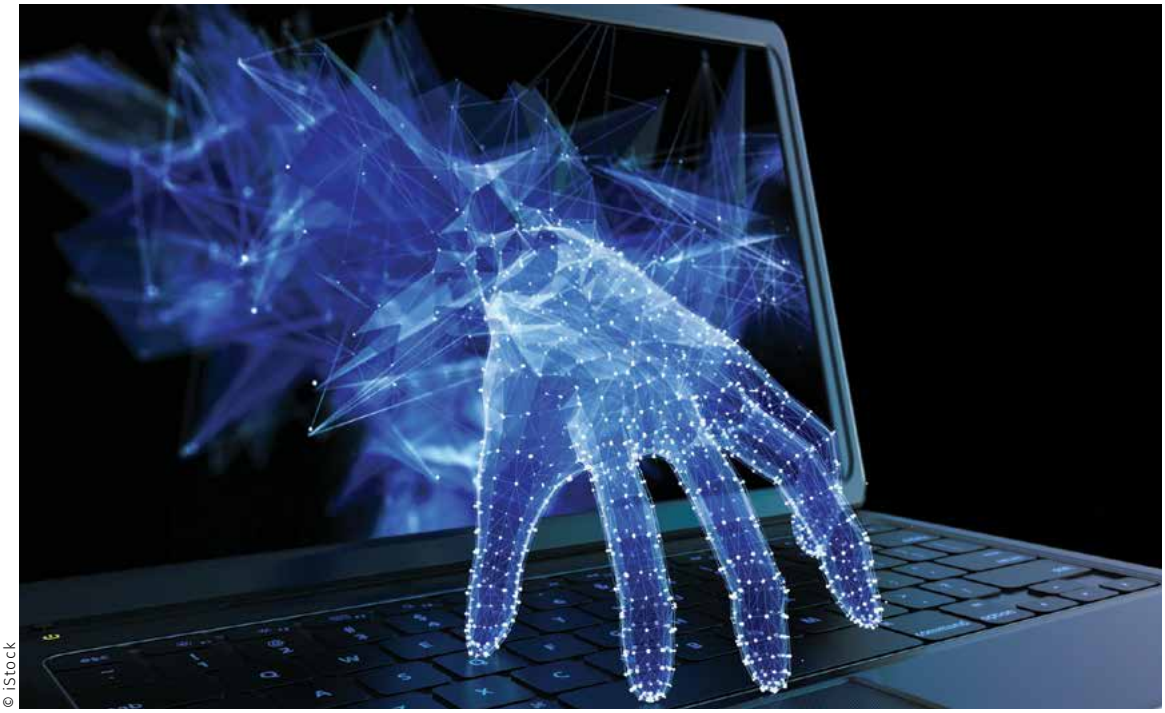
The Ministry of National Defence will continue to organise national cyber security exercises on a regular basis and will promote continuous improvement of the cyber security skills not only in the national but international cyber security exercises as well.

13. The European Union (EU) and the North Atlantic Treaty Organisation (NATO) acknowledge that cyberspace has been increasingly used as a separate military space or as a tool of hybrid warfare. Cyber tools may be used to sabotage activities of a country's critical information infrastructure (e.g., the cyber-attack which took place in one of Iran's nuclear energy objects in 2010), might adversely affect national and public security (e.g., the cyber-attacks on Ukraine's power plants in 2015 and 2016), economy and social welfare. For this reason, protecting the national cyberspace is a matter of national security for every country.

In accordance with the decision adopted during the NATO Warsaw Summit 2016 where cyber space was recognised as the fifth domain of warfare the Lithuanian Armed Forces have become the main cyberspace defence entity for the Republic of Lithuania. The strengthening of cyber defence in order to prevent military cyber threats and effectively manage cyber incidents is a prerequisite for ensuring vital and primary interests of national security. To fulfil the objectives set for the Lithuanian Armed Forces, national cyber defence capabilities will be developed by ensuring interaction between the Lithuanian Armed Forces and the country's civil capabilities, also capabilities of the Lithuanian Armed Forces to ensure reliable deterrence of aggressors in cyber space. In case of failure to ensure effective deterrence, the Lithuanian Armed Forces would defend the Republic of Lithuania by using military cyber security measures acting autonomously and in cooperation with allies.

14. **Objectives for achieving the first target of the Strategy:**

14.1. ***The first objective of the first target*** is to develop a systematic approach to cyber security and preventive activities.	This objective will be accomplished by improving the methods of cyber security risk identification, evaluation and forecast; by building up a picture of cyber security identification and a risk map to reveal the risks typically encountered in particular sectors; by establishing regional cyber security centre and state-controlled electronic communications network with a set of cyber security measures, linking state and municipal institutions, agencies and state companies, which perform state mobilisation tasks for ensuring vital state functions; by carrying out surveys on cyber security state, progress reports or maturity assessments; by implementing other measures and actions in order to enhance cyber security level and preventive activities.
14.2. ***The second objective of the first target*** is to improve the efficiency of the cyber security policy making and implementation by reducing administrative burden falling on cyber security entities.	This objective will be implemented by improving legal framework in the field of cyber security; by preparing standardised but differentiated cyber security requirements; by analysing best practice, standards applicable to ensuring cyber security; by encouraging cyber security entities to follow such standards; by establishing a national integrated crisis management mechanism to ensure cooperation among concerned parties at all levels; by updating the cyber security risk assessment system; by assessing the methodological possibilities to monitor and control the funds which are necessary to ensure cyber security while establishing priorities for the funds' allocation and use; by implementing any other measures of cyber security policy making and implementation.
14.3. ***The third objective of the first target*** is to promote national cyber security exercises and participation in international exercises.	This objective will be implemented by periodically organising complex national cyber security exercises and participating in international cyber security exercises organised by the EU, NATO and other countries; by incorporating lessons learned from national and international exercises into management of situations, incident assessment, information communication and other activities.
14.4. ***The fourth objective of the first target*** is to develop cyber defence capabilities of the country.	This objective will be achieved by ensuring effective interaction between the Lithuanian Armed Forces and civilian cyber defence capabilities; by developing cyber defence capabilities; and by providing assistance to other state and municipal institutions and agencies.



© iStock

Cybercrimes

15. **The second target of the Strategy** is to ensure the prevention and investigation of cybercrimes.

16. Cybercrimes have a negative impact on the global economy. According to research[2], global damage caused by cybercrimes amounts to hundred billions euros a year and has been increasing. Persons committing cybercrimes are interested not only in financial details, but also in data, in general. For this reason, the number of crimes that undermine electronic data and information system security specified in Chapter XXX of the Criminal Code of the Republic of Lithuania has also been steadily growing. According to the data of the Institutional Register of Crimes, in 2017, 594 cybercrimes were recorded; in 2016, 336 offences were recorded. As the European Cybercrime Centre (EC3) operating within the European Police Office (hereinafter referred to as the "EC3") states, cybercrimes are most often encountered by those European Union Member States that have a well-developed broadband infrastructure and well-functioning online payment systems.[3]

17. Referring to the data of a survey conducted by PwC in 2018 (*Global Economic Crime Survey 2018*), in 2018, fraud crimes committed in cyberspace were among the most common crimes which caused the most damage to private sector entities. EC3 forecasts that the rapid development of ICT and methods of social engineering, among other reasons, will increase the number of cybercrimes. Moreover, cybercrimes which do not necessarily involve the use of ICT, for instance, fraud or extortion, are "going digital". In order to commit cybercrimes or to conceal their traces, the latest ICT solutions, cryptocurrencies and services offered in anonymous networks are used.

18. The company Cybersecurity Ventures calculated in 2017 that the financial damages caused by cybercrimes using malware have been increasing each year. Additionally, they forecast that by the end of the year 2019, the world would suffer the damage of more than USD 11 billion due to the spread of ransomware. EC3 predicts that this trend will continue due to the increase of the Internet of Things (IoT) devices. Although malware is only one type of cybercrimes, the European Union Agency for Network and

[2] Center for Strategic and International Studies, M cAfee (2018). *Economic Impact of Cybercrime – No Slowing Down,* Cybersecurity Ventures, Herjavec Group (2017). *2017 Cybercrime Report.*

[3] Europol's European Cybercrime Centre (EC3) (2017). *2017 Internet Organised Crime Threat Assessment (IOCTA)*

Information Security (ENISA) in its Threat Landscape Report 2017 which was published in 2018 indicated that malware is the most frequent cyber threat that has prevailed in recent years.

19. Crimes related to the sexual exploitation of children in cyberspace are considered to be the most harmful and injurious cybercrimes, the spread of which is prompted by rapidly developing ICT and its potential. According to the Lithuanian national criminal records register and the Europol, such crimes have been increasing and spreading in Lithuania[4] and in Europe.[5] In seeking to prevent crimes related to the sexual exploitation of children, Lithuania has transposed Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, which replaced Council Framework Decision 2004/68/JHA (OJ 2011 L 335, p. 1) into national legislation and on 6 November 2012 ratified the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse dated 25 October 2007.

20. In order to combat international cybercrimes, it is important to develop close cross-border cooperation and exchange of information, to maintain and deepen agreements and membership-based relationships. To this end, it is necessary to have the strong political will to effectively fulfil international obligations and comply with international standards to ensure cyber security and combat cybercrimes. To express a clear political will, Lithuania ratified the Convention on Cybercrime of the Council of Europe of 23 November 2011 (hereinafter referred to as the "Budapest Convention") and its additional protocols. In addition, Lithuania transposed Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems, replacing Council Framework Decision 2005/222/JHA (OJ 2013 L 218, p. 8) into national legislation. Obligations are successfully fulfilled on both legal and practical levels by cooperating with the International Criminal Police Organisation (hereinafter referred to as the "INTERPOL") and the INTERPOL Global Complex for Innovation (IGCI), the Europol and EC3 and the European Union's Judicial Cooperation Unit (Eurojust). Moreover, Lithuania has taken part in the activities of continuously operating contact points of the network specialising in the field of cybercrime investigation which was founded on the basis of the European Judicial Network (EJN) and in accordance with the Budapest Convention.

21. Since cybercrimes continue to evolve, personnel of law enforcement authorities must be equipped with necessary skills to perform their allocated tasks. The appropriate competences of employees and their superior officers of the prosecution authorities and the courts must be taken into account as well. In relation to the investigation of cybercrimes, the competence of law enforcement authorities is crucial in order to detect, capture and investigate electronic evidence.

[4] According to the data of the Lithuanian national criminal records register, in 2016, 123 crimes were registered as per definition provided in Article 309(2) of the Criminal Code, in 2017 – 132.

[5] European Union Agency for Law Enforcement Cooperation (Europol) (2017). *Europol Review 2016–2017.*

22. **Objectives for achieving the second target of the Strategy:**

22.1. ***The first objective of the second target*** is to develop capabilities and capacities of the country for combating cybercrimes.	This objective will be attained by improving the legal framework, by further strengthening the professional capacity of law enforcement authorities, by creating information and/or analysis systems, putting in practice advanced operational methods, procedures and technical tools specifically designed to combat cybercrimes.
22.2. ***The second objective of the second target*** is to strengthen the prevention and control of cybercrimes.	This objective will be implemented by promoting the society's culture of self-protection and responsible behaviour in cyberspace; by increasing the operational effectiveness of law enforcement authorities and ensuring effective international cooperation while investigating cybercrimes; by developing effective cooperation between law enforcement authorities and academia, private and public sector representatives and society.

© shutterstock

Cyber Security Culture and Innovation

23. **The third target of the Strategy** is to promote cybersecurity culture and innovation.

24. It is impossible to avoid cyber incidents in the modern-day world, even if all existing cyber security measures are to be applied. For this reason, public and private sector representatives must improve cybersecurity culture of their employees. According to IBM report published in 2017[6], the number of cyber incidents caused due to employee negligence has been growing (in 2017, the number of such cyber incidents constituted more than 20%, in 2016 – 15%). More than 30% of these cyber incidents happened because employees opened malicious links or documents sent to them via email. In Lithuania, the number of emails created using social engineering methods has also been rising.[7]

25. According to the European Innovation Scoreboard dated 2018, private sector representatives in Europe have been increasing their focus on ICT training of their employees. While Europe as a whole has an average index of 21%, in Lithuania it is slightly greater than 10%. Civil servants in Lithuania are given opportunities to improve their skills in the field of cyber security and the number of civil servants who have taken cybersecurity courses is growing annually. According to Civil Service Department, there were 146 such civil servants in 2015, 249 – in 2015 and 289 – in 2017. Routine and regularly updated training courses for private and public sector employees would increase employees' duty of care as well as the overall cybersecurity culture.

26. Efficient and regular dissemination of information on the latest cyber incidents and other factors that may cause personal data breach or pose a risk of becoming a victim of cybercrime is a key measure for strengthening cybersecurity culture of the Lithuanian people. According to the special Eurobarometer survey 464a which reveals Europeans' attitude towards cybersecurity, only 16% of the internet users in Lithuania believe that the risk of becoming a victim of a cybercrime has not been increasing (the European Union average is 11%). Nevertheless, as 49% of the internet users in Lithuania

[6] *IBM. IBM X-Force Threat Intelligence Index 2018 (2018).*

[7] National Cyber Security Centre under the Ministry of National Defence (2018). *National Cyber Security Status Report 2017.*

believe that they are not sufficiently aware of the full risk of cybercrimes (the European Union average is 51%), the dissemination of information should be increased in this regard.

27. There have been a number of surveys and forecasts conducted worldwide which indicate that people lack cyber security skills[8] and that this will continue to be true in the future. Quality public education which corresponds with the needs of labour market is a tool that can contribute to professional competence. Presently, cyber security programmes are offered by four universities in Lithuania; yet according to the results of the survey titled "The ICT Specialists in Lithuania: Situation in the Labour Market and Employers' Needs" that was carried out by the association Infobalt and the public institution Invest Lithuania, current labour market needs are not met. In order to reduce the gap between supply and demand of cybersecurity specialists, the existing cybersecurity study programmes must be improved and new study programmes shall be established.

To boost cybersecurity culture, children and pupils should be provided with the fundamental knowledge of cybersecurity under nursery, preschool, primary and/or secondary education programmes since ICT is used to ensure educational and learning processes.

In the context of implementing programme of the Government of the Republic of Lithuania on reorganisation of the system of teachers' up-skilling and training, efforts should be made to improve teachers' qualifications in the area of cybersecurity. Having the opportunity and ability to expand and deepen their cybersecurity knowledge, teachers of different educational areas would not only be able to educate young people better, but would contribute to the development of knowledge and innovation based society and further cybersecurity awareness raising as well.

28. Many cybersecurity experts[9] estimate that by the year 2019, there will be at least 1.5 million employment vacancies worldwide for cybersecurity professionals. The study "ICT Specialists in Lithuania: Situation in the Labour Market and Employers' Needs", conducted by the association Infobalt and public organisation Invest Lithuania in 2018, revealed that while there are 22,600 ICT specialists in Lithuania, about 13,300 more would be needed within the following three years. Regrettably, researchers provided no details about this shortage of cybersecurity specialists in Lithuania, but it may be assumed that they are in high demand. To address this shortage, cybersecurity skills that cybersecurity specialists are expected to have in Lithuania first must be identified because the demand for cybersecurity professionals may vary in different countries and problems related to the lack of cybersecurity skills may differ according to the conclusions of studies carried out in other countries[10].

29. With regard to rapid development of cyberspace, various opportunities for innovation, which, in turn, drives economic and productivity growth, have emerged. This prompts the creation of new and better jobs, increases social mobility and responds to social and security challenges globally.

Lithuania joined the European Union a relatively short time ago, for this reason, there is neither long tradition of cybersecurity scientific research nor education, whereas they are present in other EU Member States. The European Union has provided Lithuania with a great opportunity to promote investment in scientific research through the general research and innovation programme Horizon 2020 (2014–2020). Through this programme, Lithuania may contribute to the development of the digital economy and defence policy on both the national and the EU level. However, all efforts of the state in this direction must be focused on support measures that promote international networking in finding potential employees and partners. This would stimulate private sector investment in the R&D and innovation areas, new technologies, tools and services and in the cyber security area as well. The designing of innovative cyber security products would not only provide additional support and leverage for the competitiveness of the Lithuanian industry, but it is a key factor in responding to modern cyber incidents. It is also important to encourage Lithuania's academics to participate in joint international academic publications in the field of cyber security, to attract as many students as possible to high-level R&D projects that focus on cyber security, to promote public-private partnership and academia cooperation and to increase the number of foreign doctoral students in the area of cyber security.

30. According to the data from the European Innovation Scoreboard 2018, in comparison with other EU Member States, Lithuania is a moderate innovator but it has advanced considerably in terms of innovation and improvement of the ecosystem of innovation.[11] In the European Union, the private sec-

[8] ISACA. *State of Cybersecurity 2018 (2018),* Information Security Community on LinkedIn, (ISC)². *Cybersecurity Trends. 2017 Spotlight Report (2017).2017 Spotlight Report (2017).*

[9] Silensec. *Addressing the Cyber Security Skills Gap (2017).*

[10] Indeed. *Indeed Spotlight: The Global Cybersecurity Skills Gap (2017),* Information Security Community on LinkedIn, (ISC)². *Cybersecurity Trends. 2017 Spotlight Report (2017.)2017 Spotlight Report (2017).*

tor still allocates insufficient resources to innovation compared to its rivals beyond European Union borders. No reliable measurements of the cyber security market have yet been carried out in Lithuania, but it is acknowledged that this market has been growing and, for this reason, innovation would help strengthen Lithuania's competitive position in the development of new innovative products and services. This synergy could be attained by combining initiatives of innovation and general national policies while promoting long-term science, technology and innovation development.

31. Lithuania's regulatory and supervisory environment is favourable to financial services and promotes innovation in the finance sector. Pursuant to the data of Lithuania Fintech Report 2017, there were 117 financial technology enterprises operating in Lithuania in 2017. The development of financial technology is one of the strategic activity directions for the Bank of Lithuania and its activity in one of the most promising and prospective areas of financial technology innovation, blockchain technology, will further drive innovation in financial technology field.

32. **Objectives for achieving the third target of the Strategy:**

32.1. ***The first objective of the third target*** is to develop scientific research and activities that create high added value in the area of cyber security.	This objective will be implemented by creating favourable conditions for the creation of new, advanced cybersecurity initiatives; by promoting growth of the cybersecurity market, by expanding export of cybersecurity services to foreign markets; by developing cyber security sector of financial technology and by conducting research.
32.2. ***The second objective of the third target*** is to develop creativity, advanced capabilities and cyber security skills and competence that meet market needs.	This objective will be implemented by creating a cybersecurity competence model; by establishing cybersecurity competence standards; by developing systems of training, accreditation and certification oriented towards the needs of the labour market; by attracting, nurturing and retaining talent; by creating training and testing environments for cybersecurity; by teaching newcomers and providing retraining opportunities for ICT workers; and by training employees working with sensitive data.
32.3. ***The third objective of the third target*** is to promote public, private, and academic partnerships while creating innovation in cybersecurity field.	This objective will be implemented by identifying the common needs of the private and public sectors and their importance in relation to scientific cybersecurity research; by creating technical measures, methods and other resources; and by developing the requisite expertise for solving cybersecurity problems or fulfilling any other specific tasks for cybersecurity.

[11] European Commission. *2018. The European Innovation Scoreboard (2018).*

Private-Public Partnership

33. **The fourth target of the Strategy** is to promote close PPP.

34. In modern states, in which the broadband infrastructures are well developed, public sector representatives as well as managers of critical information infrastructures who are often private sector representatives, are not always able to combat cyber incidents independently. Thus cooperation between public and private sectors becomes inevitable in order to ensure comprehensive cybersecurity. The PPP success factor is a fully-fledged partnership, which entails trust and mutual benefit. Thus public and private sectors should strive to work together to this end.

35. The Cyber Security Council set up following the approval of Resolution No. 422 of the Government of the Republic of Lithuania of 23 April 2015 "On the Approval of Establishment of a Cyber Security Council and its Rules of Procedure" is an example of PPP on a political level. All efforts must be made to effectively enjoy the rights of a Cyber Security Council that are defined in the Law on Cyber Security.

36. To ensure PPP, the Cyber Security Information Network (hereinafter referred to as the "Network") is used. The aim of the Network is information sharing, exchange of cybersecurity recommendations, instructions, and technical solutions, and other measures which could help ensure cybersecurity of the Network members. It is necessary to integrate appropriate measures in the Network for more effective and trusted cooperation among the Network members.

37. The advantages of ICT are beyond question in the 21st century, but the issue of how to effectively address vulnerabilities in ICT systems arises. Security vulnerabilities may be detected by the persons who may have different goals; however, in order to develop a responsible disclosure approach, it is important to give a particular opportunity to a person, who has been able to identify a vulnerability and wants to contribute to security of ICT systems, to cooperate with cybersecurity

entities whose security vulnerability was disclosed. Establishment and public announcement of a formalised procedure for responsible disclosure would contribute to the protection of cybersecurity entities from possible damage caused by cyber incidents or could considerably diminish such damage. This would also enhance cybersecurity of the country and would give more opportunities for PPP.

38. **Objectives for the attainment of the fourth target of the Strategy:**

38.1. ***The first objective of the fourth target*** is to improve coordination of PPP.	This objective will be implemented by creating a sustainable PPP model in the field of cyber security; by identifying responsibilities and capabilities related to cybersecurity; by improving effective exchange of relevant information about cyber threats, cyber incidents and lessons learned; by supporting an early warning system; and by creating new or improving the existing communication techniques and processes.
38.2. ***The second objective of the fourth target*** is to increase cybersecurity maturity of small and medium-sized enterprises (hereinafter SMEs).	This objective will be implemented by encouraging SMEs to verify their cybersecurity state and address cybersecurity gaps.
38.3. ***The third objective of the fourth target*** is to develop a responsible vulnerability disclosure practice.	This objective will be implemented by establishing operational principles, methods, technical capabilities or other measures designed for this purpose.

© iStock

International Cooperation

39. **The fifth target of the Strategy** is to enhance international cooperation and ensure the fulfilment of international obligations in the field of cybersecurity.

40. Lithuania's national security and the prosperity of the Lithuanian society depend directly on stable, easily and freely accessible and secure cyberspace. Considering the fact that modern cyber threats and risks can easily cross national borders, Lithuania will seek to strengthen its national cybersecurity by actively cooperating with bilateral and multilateral partners and by participating in international forums designed for resolving problems related to cybersecurity and internet governance.

41. Lithuania is eager to become an active partner in the international community which seeks to resolve cyber security and internet governance problems. Lithuania is active in building cooperation with partners and allies by signing an international agreement for legal regulation of cyberspace which shall comply with the provisions of international law, standards and principles that apply to activities in cyberspace in relation to protection of the open Internet principle as well as other principles on fundamental freedoms and human rights.

Lithuania advocates more close and harmonious cooperation with NATO and the European Union in the cybersecurity field with the aim of avoiding overlap of functions and activities. Lithuania shall also strengthen bilateral political and technical cooperation with other countries which adhere to the principles of democracy, especially, with the United States of America.

42. **Objectives for the fulfilment of the fifth target of the Strategy:**

42.1. ***The first objective of the fifth target*** is to develop international, cross-border cooperation, including cooperation with the countries of the Baltic region in the field of cyber security.	This objective will be fulfilled by participating in the activities of the European Union, NATO, the United Nations, the Organisation for Security and Co-operation in Europe (OSCE), organisations of the Baltic region and other international organisations.

42.2. ***The second objective of the fifth target*** is to strengthen international cybersecurity capabilities and capacities.	This objective will be implemented by initiating and leading the Permanent Structured Cooperation in Security and Defence Policy (PESCO) project for improvement of cooperation in security and defence area in terms of those EU member states that have military capabilities which meet higher criteria and are bound by greater commitments.
42.3. ***The third objective of the fifth target*** is to further develop the dialogue with the United States of America in the field of cyber defence and to strive for the involvement of the United States of America in Lithuania's cybersecurity projects.	This objective will be implemented by developing bilateral cooperation between Lithuania and the USA at technical and political levels and by pursuing activities that would strengthen Lithuania's cyber defence and cybersecurity capabilities.

3

Implementation of and Responsibility for the Strategy

43. The Government of the Republic of Lithuania shall approve an inter-institutional operational plan where particular measures and funds will be foreseen in order to implement the targets and objectives of the Strategy. The Ministry of National Defence shall coordinate the drafting of this plan jointly with the NCSC. Ministries, other state or municipal authorities, agencies or organisations specified in the inter-institutional operational plan of the Strategy shall, within the limits of their competence, participate in the implementation of the Strategy (hereinafter referred to as the "Strategy Implementers").

44. Non-governmental organisations, representatives of public and private stakeholders and Lithuania's academia may contribute to the Strategy's implementation and the fulfilment of its goals and objectives.

45. Each year the Strategy shall be implemented using funds allocated from the Republic of Lithuania state budget, municipal budgets, the European Union and other international funds, and other legally obtained sources. The responsibility for planning of the required financial resources shall be assumed by the Strategy Implementers and shall be carried out according to the principle of subsidiarity as defined in the Law on Cybersecurity.

46. The accomplishment of the Strategy's goals shall be assessed according to the criteria for implementation of the Strategy and the targeted values indicated in the Annex to the Strategy. Monitoring and assessment of the implementation of the Strategy will be also based on publicly available data derived from the Department of Statistics, Eurostat, sociological surveys and other surveys. The Ministry of National Defence, the NCSC and the Cyber Security Council shall monitor the results of the Strategy's implementation.

47. The Strategy Implementers shall provide the NCSC with information on the course of the implementation of the Strategy and its effectiveness along with supporting documents after the end of a year but no later than before 15 January of the following year. This information may be accompanied where appropriate with proposals for revision of the Strategy or its implementation documents. If requested by the NCSC, the Strategy Implementers are obliged to submit any other information required for monitoring of the Strategy implementation results. All stakeholders are entitled to propose updates to the provisions of the Strategy at any time during its implementation.

48. After receipt of the information specified in Paragraph 47 of the Strategy, the NCSC shall provide the Ministry of National Defence with processed data on the state of implementation of the Strategy's targets and objectives of the previous year and shall also forward its suggestions and indicated problematic issues which hinder the implementation of the Strategy no later than 1 February of the current year.

49. The Ministry of National Defence shall summarise the information received over the previous year and the data about the course of implementation as well as efficiency of the Strategy by 1 March each year. Aggregated information on the annual implementation of the Strategy shall then be presented to the Cyber Security Council and submitted to the Government. The Government shall report to the Seimas of the Republic of Lithuania with regard to the implementation of the Strategy annually by providing an Annual Report on the State of National Security and Development.

50. All public information related to the annual and final Strategy implementation assessments shall be announced on the NCSC website.

51. The NCSC shall draft a final assessment of the implementation of the Strategy six months before the Strategy's implementation deadline and shall submit it to the Ministry of National Defence. It shall be then forwarded to the Cyber Security Council and the Government.

Annex to the National Cyber Security Strategy

Criteria for Assessing the Implementation of the National Cyber Security Strategy and the List of Targeted Values

Item Number	Name of the Evaluation Criterion	Value of the Evaluation Criterion			Responsible state institution
		Initial known value in 2017	2021	2023	
	The main purpose of the National Cyber Security Strategy (hereinafter referred to as the "Strategy") is to provide the Lithuanian people with the opportunity to explore the potential of information and communications technology (ICT) by identifying cyber incidents timely and effectively, by preventing cyber incidents and their recurrence, and by managing the impact of cybersecurity breaches.				
	Position of the Republic of Lithuania in the global cyber security index (not lower than specified)	57	30	20	Ministry of National Defence
1.	Level of cyber incident threat (not higher than specified)	3.4	3.2	3	Ministry of National Defence
	The first target of the Strategy to strengthen cyber security in the country and to develop cyber defence capabilities.				
2.	Percentage of cyber security entities that meet cyber security requirements (not lower than specified)	*	35	50	Ministry of National Defence
3.	Percentage of public sector websites that are difficult to hack (not lower than specified)	25	28	32	Ministry of National Defence
4.	Percentage of managers of critical information infrastructure and state information resources that participate in national cyber security exercises (not lower than specified)	42	60	70	Ministry of National Defence
5.	Percentage of modernised cyber security and cyber defence capabilities of the state (not lower than specified)	Restricted (R)	R	R	Ministry of National Defence
	The second target of the Strategy is to ensure the prevention and investigation of cybercrimes.				
6.	Percentage of police officers, public prosecutors, specialists and experts who are involved in the investigation of cybercrimes and have completed respective training (not lower than specified)	*	70	90	Ministry of National Defence in cooperation with the Strategy Implementers
7.	Number of created or implemented information/analysis systems, procedures and technical tools specifically designed to combat cybercrimes, in units (not lower than specified)	*	2	5	Ministry of National Defence in cooperation with the Strategy Implementers

Item Number	Name of the Evaluation Criterion	Value of the Evaluation Criterion			Responsible state institution
		Initial known value in 2017	2021	2023	
8.	Number of projects intended for the prevention and control of cybercrimes, expressed in units (not lower than specified)	2	2	2	Ministry of National Defence in cooperation with the Strategy Implementers
9.	Number of participations in international events and working groups for the prevention and investigation of cybercrimes, expressed in units (not lower than specified)	12	14	15	Ministry of National Defence in cooperation with the Strategy Implementers
10.	Number of participations in international operations to investigate cybercrimes (not lower than specified)	3	4	6	Ministry of National Defence in cooperation with the Strategy Implementers
	The third target of the Strategy is to promote cybersecurity culture and innovation.				
11.	Total number of projects that have promoted innovation in the cybersecurity field since 2018	0	5	10	Ministry of National Defence in cooperation with the Strategy Implementers
12.	Amount of investment in the promotion of digital literacy culture and the development of knowledge related to cybersecurity and scientific research, thousand Eur (not lower than specified)	*	1, 000	2, 000	Ministry of National Defence in cooperation with the Strategy Implementers
13.	Number of persons who have obtained qualifications in cyber security, in units (not lower than specified)	33	200	400	Ministry of National Defence in cooperation with the Strategy Implementers
14.	Percentage of public servants and employees of public institutions who were trained via the module of the State Civil Servants' Register and Public Service Management Information System (not lower than specified)	0	10	70	Ministry of National Defence in cooperation with the Strategy Implementers
	The fourth target of the Strategy is to promote close PPP.				
15.	Number of PPP models in the field of cyber security, expressed in units	0	0	1	Ministry of National Defence in cooperation with the Strategy Implementers
16.	Percentage of managers of state information resources and of critical information infrastructures incorporated into the Cyber Security Information Network (not lower than specified)	36	86	90	Ministry of National Defence
17.	Number of measures designed to improve the cybersecurity status of SMEs, expressed in units (not smaller than specified)	0	4	6	Ministry of National Defence in cooperation with the Strategy Implementers
18.	Number of measures designed to develop a responsible vulnerability disclosure practice, expressed in units (not smaller than specified)	0	1	2	Ministry of National Defence in cooperation with the Strategy Implementers

Item Number	Name of the Evaluation Criterion	Value of the Evaluation Criterion			Responsible state institution
		Initial known value in 2017	2021	2023	
	The fifth target of the Strategy is to enhance international cooperation and ensure the fulfilment of international obligations in the field of cybersecurity.				
19.	Percentage of participation in the meetings, forums or other events related to cyber security matters organised by the EU, NATO and the Baltic Region to which invitations were received (not lower than specified)	25	50	70	Ministry of National Defence in cooperation with the Strategy Implementers
20.	Percentage of participation in the meetings of international organisations for cyber incidents' investigation to which invitations were received (not lower than specified)	70	85	100	Ministry of National Defence
21.	Number of cooperation agreements signed with international organisations, European Union Member States, NATO Member States, countries in the Baltic region and other countries in the field of cybersecurity, in units (not lower than specified)	2	1	2	Ministry of National Defence in cooperation with the Strategy Implementers

* Initial value of a respective criterion for the assessment of implementation of the Strategy is not known because authorities which coordinate the compliance with a certain assessment criterion have no information on the values of these assessment criteria. Data on the value of an assessment criterion will be collected in 2019.

NATIONAL CYBER SECURITY STRATEGY

Managing editor Aušra Pipirienė
Editor Julija Zujevaitė-Rinė
Graphic designer Aida Janonytė

30.05.2019. Circulation 40 units. Order GL-414.
Ministry of National Defence of the Republic of Lithuania,
Totorių St. 25/3, LT-01121 Vilnius
Layout by the Visual Information Section
of the General Affairs Department of the Ministry of National Defence,
Totorių St. 25/3, LT-01121 Vilnius.
Printed by the Military Cartography Centre of the Lithuanian Armed Forces,
Muitinės St., Domeikava, LT-54359 Kaunas District.

The bibliographic information about the publication is
available in the National Bibliographic Data Bank (NBDB)
of the Martynas Mažvydas National Library of Lithuania.

ISBN 978-609-412-164-7