GOVERNMENT OF THE REPUBLIC OF LITHUANIA

RESOLUTION
ON THE APPROVAL OF THE NATIONAL CYBER SECURITY STRATEGY

13 August, 2018 No. 818
Vilnius

In accordance with Article 5(1) of the Republic of Lithuania Law on Cyber Security and implementing Article 7(1) of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ 2016 L 194, p. 1), the Government of the Republic of Lithuania hereby r e s o l v e s t o :

1. approve the National Cyber Security Strategy (attached);

2. commission the Ministry of National Defence of the Republic of Lithuania to submit a draft Interinstitutional Action Plan for the implementation of the National Cyber Security Strategy to the Government of the Republic of Lithuania for approval before 2 November 2018;

3. offer to non-governmental organisations, representatives of public and private sector stakeholders and Lithuanian science and education institutions to participate in the implementation of the National Cyber Security Strategy.

Prime Minister Saulius Skvernelis

Minister of National Defence Raimundas Karoblis

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

NATIONAL CYBER SECURITY STRATEGY

CHAPTER ONE
GENERAL PROVISIONS

1. The National Cyber Security Strategy (hereinafter referred to as the "Strategy") sets out the main national cyber security policy orientations in public and private sectors. The implementation of the Strategy is aimed at strengthening cyber security of the state and the development of cyber defence capabilities, at ensuring prevention and investigation of criminal offences committed using the objects of cyber security (hereinafter referred to as the "criminal offences in cyberspace"), at promoting the culture of cyber security and development of innovation, at enhancement of a close collaboration between public and private sectors as well as international cooperation and ensuring the fulfilment of international obligations in the field of cyber security in the country until 2023.

2. The strategy has been drawn up with the environmental analysis, data of the conducted research, suggestions of the representatives of public and private sectors taken into account and 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"), of 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", of the Law of the Republic of Lithuania on Cyber Security, of the communications and recommendations by the European Parliament, the Council, and the European Commission in the field of cyber security, as well as of 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 has also become one of the key guidelines referred to by 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.

CHAPTER TWO
TARGETS AND OBJECTIVES OF THE STRATEGY, EVALUATION CRITERIA AND THEIR VALUES

4. The main purpose of the strategy is to provide the Lithuanian society with the opportunity to exploit the potential of information and communications technology (ICT) by identifying cyber incidents in an effective and timely manner, preventing their occurrence and spread, and managing consequences resulting from cyber incidents.

SECTION ONE
STATE'S CYBER SECURITY AND CYBER DEFENCE CAPABILITIES

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

6. Like other countries of the world in which the potentials of the ICT are exploited and which have a perfectly well developed broadband infrastructure, Lithuania has become attractive not only to individual persons, to their groupings and organised groups but also to the countries specified in the reports of annual national security threat assessments of 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) which pose threat to Lithuania's national security and conduct adverse activities in the global and Lithuanian cyberspace. Data collected by the National Cyber Security Centre under the Ministry of National Defence (NCSC), SSD and SID has revealed that Lithuania continuously encounters various types of cyber incidents aimed at infringement on the national information resources and critical information infrastructure; according to forecasts, the number and extent of cyber incidents are not likely to reduce in the future[1].

7. According to the data of the Report on the State of National Cyber Security 2017, in 2017, the National Electronic Communication Networks and Information Security Incidents

[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). *Report on the State of National Cyber Security 2017*.

Investigation Unit – Computer Emergency Response Team in Lithuania (CERT-LT) – processed as many as 54, 414 cyber incidents. In 2017, the number of recorded cyber incidents was 10% higher than in 2016. The Lithuanian national information resources remain the primary target of cyber-espionage attacks; nonetheless, critical information infrastructure of the private sector and other enterprises which are of strategic or great importance to the national security is no exception either. Applying technical cyber security measures the NCSC has identified that the biggest number of cases of proliferation of malicious software was in the sectors of energy (27%), public security and legal order (22%) and foreign affairs and security policy (21%). Compared to 2016, malicious software mostly proliferated in the areas of public security and legal order, foreign affairs and security policy, and energy. The situation of cyber security in the country is also strongly affected by the state of websites of public sector which, based on the data of the Report on the State of National Cyber Security 2017, deteriorated in 2017.

8. The annual reports of the NCSC, SSD and SID provide information on the extent of proliferation of cyber incidents which shows that every cyber security subject faces situation where a decision has to be made on how much time, money or any other resources might be needed to protect the existing communication and information systems or provided services. Cyber security subjects perform security risk assessment but risk assessment is often conducted formally only so as to comply with the requirements of legal acts or provision of internationally recognised standards.

The *Risk Analysis Manual* published by the Ministry of the Interior of the Republic of Lithuania reflects the progress and advancement of the risk assessment by research and innovation tools of the time, however, the provisions of the security risk assessment methodology have gradually changed and control environment assurance has transformed into all-encompassing activity risk assessment of an organisation.

9. Individual assessment processes in terms of different security areas in Lithuania have already reached the point of maturity, however, on the national level, the security risk assessment culture and cyber security risk assessment are still fragmentary. There is a lack of analysis on cyber threats and gaps in security as well as full integration into activity risk assessment processes. Furthermore, rapid development of ICT results in the staff responsible for cyber security lacking knowledge, skills and practice.

10. To improve the culture of cyber security policy development and implementation, to update cyber security risk assessment and other requirements, the following significant changes took place in the field of cyber security in 2018:

10.1. Recast provisions of the Law on Cyber Security helped improve the organisation, management and control of the cyber security system, specified competence, functions, rights and duties of authorities which develop and implement cyber security policy, duties and responsibility of cyber security agents, and established additional cyber security assurance measures.

10.2. The functions of regulation and safeguarding the security of state information resources, of the activities of public communications networks, public electronic service

providers and electronic information hosting providers were mustered up which enabled the state to ensure systematic monitoring of cyber space, control of and responsibility for cyber incidents occurring in communication and information systems of cyber security entities; the NCSC has become the only agency in Lithuania to organise cyber incident management in the country and provide help and assistance to state institutions, business and residents under the principle of one stop shop.

11. Consolidation of capabilities is aimed at developing an integral cyber security management system in Lithuania which would represent a systematic approach to the security management planning in any field, promote orientation of cyber security entities to security management quality assurance, reduce administrative burden falling on cyber security entities, ensure the systematicity of assessment and evidence-based security management culture, help optimise the planning of security expenditure. Among the aims is the target to ensure 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 and provide consultations on the topics of cyber security as well as 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 the representatives of cyber security entities were organised – they were familiarised with the requirements of legal acts in the area of cyber security. Participants of the exercise had trainings aimed at containing and resisting cyber-attacks against critical communication and information systems and ensure the functioning of such systems.

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

13. The European Union and the North Atlantic Treaty Organisation (NATO) acknowledge that the cyber space in some cases has become a separate military space or one of the tools of hybrid warfare. Cyber measures may be used to sabotage operation of a country's critical information infrastructure (e.g., a cyber-attack which took place in one of Iran's nuclear energy objects in 2010), might negatively affect the security of a country and its society (e.g., cyber-attacks in Ukraine's power plants in 2015 and 2016), undermine economy and social welfare; for this reason, the security of the national cyber space is a legitimate national security interest of every country.

In accordance with the decision adopted in NATO Warsaw Summit 2016 with regard to recognition of cyber space as the fifth warfare domain, the Lithuanian Armed Forces have become the main cyber space defence entity of the Republic of Lithuania. The strengthening of cyber defence so as to prevent military cyber threats and to effectively manage cyber incidents is

one of the prerequisites for ensuring vital and primary interests of a country's national security. To fulfil the objectives set for the Lithuanian Armed Forces, national cyber defence capabilities will be developed which will help ensure interaction between the Lithuanian Armed Forces and the civil capabilities of the country, also capabilities of the Lithuanian Armed Forces to ensure reliable deterrence of aggressors in cyber space, and in case of failure to deter aggressors – to independently and in cooperation with the Allies – to defend the Republic of Lithuania making use of all cyber security measures.

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 activity. This objective will be pursued by improving the ways 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 typical of individual sectors, by developing a regional cyber security centre and state-controlled electronic communications network with complex cyber security measures which would incorporate state mobilisation tasks for performing critical state functions assigned to state and municipal institutions, agencies and companies, by carrying out surveys on cyber security state, measurements of advancement or maturity assessments, by ensuring public information on cyber security state, by putting into use other measures and actions which reinforce cyber security and preventive activities.

14.2. *Second objective of the first target* is to increase the efficiency of cyber security policy development and implementation by reducing administrative burden falling on cyber security entities. This objective will be attained by improving legal regulation of cyber security, by preparing standardised but differentiable cyber security requirements, by carrying out the analysis of good practice, standards applicable when ensuring cyber security, by encouraging cyber security entities to follow such standards, by establishing a national integrated crises management mechanism, by ensuring smooth cooperation among the structures of all levels, by updating cyber security risk assessment system, by evaluating methodological potentials to conduct monitoring and control of the funds required for cyber security, by determining the priority of their allocation and use, by implementing any other measures of cyber security policy development and implementation.

14.3. *The third objective of the first strategy* is to promote organisation of and participation in international exercises. This objective will be fulfilled by periodically organised complex national cyber security exercises, by participation in the EU, NATO and other countries organised and led exercises, by incorporation of experience of national and international exercises into incident assessment, information communication and other actions.

14.4. *The fourth objective of the first strategy is* to develop cyber defence capabilities of the country. This objective will be achieved by ensuring effective interaction of the Lithuanian Armed Forces and civilian capabilities, by developing cyber defence capabilities and by providing assistance to other state and municipal institutions and agencies.

SECTION TWO

CRIMINAL OFFENCES IN CYBER SPACE

15. **The second target of the Strategy** is to ensure prevention and investigation of criminal offences in cyber space.

16. Criminal offences in cyber space have a negative impact on the world's economy. According to research[2], global damage caused by criminal offences in cyber space amounts to hundred billions euros a year; the trends are developing in a towering manner in this regard. Persons committing criminal offences are interested not only in financial details, but in all data in general. For this reason, the number of crimes which undermine electronic data and information system security specified in Chapter XXX of the Criminal Code of the Republic of Lithuania has been continuously growing (according to the data of the Institutional Register of Crimes, in 2017, as many as 594 criminal offences of this type were recorded, in 2016, there were 336 of them). As the European Cybercrime Centre (EC3) operating within the European Police Office (hereinafter referred to as the "Europol") states, criminal offences in cyber space are most often encountered by those European Union Member States which have a well-developed broadband infrastructure and have 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 offences *in* cyber space were among the most frequent crimes which cause the most considerable damage to private sector. The European Cybercrime Centre (EC3) operating within the Europol forecasts that the rapid development of ICT and methods of social engineering and other reasons are leading to the fact that the number of criminal offences in cyber space has been increasing. Besides, cyber space has been seeing an increasing number of criminal offences which do not necessarily involve the use of ICT, for instance, fraud or extortion. To carry out such crimes or to conceal their traces the latest ICT solutions, cryptocurrency are employed and criminal services, which are offered in an anonymous network, are used.

18. Cybersecurity Ventures company calculated in 2017 that damage caused by criminal offences in cyber space, where malicious software was used had been annually growing and forecast that by the year 2019, the world would suffer more than USD 11 billion damages due to the spread of ransom malware. The European Cybercrime Centre (EC3) within the Europol foresees that such harm will continue to augment, in particular, for the reason of increase in devices of the Internet of Things (IoT). Although malware is often only one of the ways for criminal offences in cyber space, the European Union Agency for Network and Information Security (ENISA), in 2018, indicated ransomware in its Threat Landscape Report 2017 as the most frequent cyber threat which had been dominating for a few years.

---

[2] Center for Strategic and International Studies, McAfee (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)*

19. Criminal offences related to sexual exploitation of children in cyber space are considered the ones of the most harmful and injurious criminal offences the spread of which is prompted by rapidly developing ICT and the increasing potentials of its use. This type of crimes in cyber space has been gaining an increasing extent and their number pursuant to the data of the Institutional Register of Crimes and the Europol has been growing both in Lithuania[4] and in Europe[5]. Seeking to prevent criminal offences related to 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, and replacing Council Framework Decision 2004/68/JHA (OJ 2011 L 335, p. 1), 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. To prevent criminal offences in cyber space which trespass the borders of countries, it is important to develop close cross-border cooperation and exchange of information, maintain and deepen relationship based on international agreements and membership. To this end, a crucial role is played by strong political will to fulfil international obligations effectively and comply with international standards to ensure cyber security and tackle crime in cyber space. Expressing its 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 and replacing Council Framework Decision 2005/222/JHA (OJ 2013 L 218, p. 8). Obligations are fulfilled successfully not only on a legal but also on a practical level by cooperating with the International Criminal Police Organisation (hereinafter referred to as the "Interpol") and the Interpol's Global Complex for Innovation, the Europol and European Cybercrime Centre (EC3) operating within the Europol as well as with 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 criminal offences in cyber space kept evolving and have gained new forms, staffs of law enforcement authorities which work in the field of investigation and prevention of criminal offences must be properly prepared to assess cyber threats, identify criminal offences in cyber space and investigate them effectively. Another important aspect is appropriate competence of employees of the public prosecutor's office and courts as well as of persons who organise activities of the said authorities and are involved in leadership. To investigate such crimes law enforcement authorities must be capable of finding, recording and investigating electronic evidence fast.

---

[4] According to the data of the Institutional Register of Crime, in 2016, as many as 123 crimed 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 to deal with criminal offences in cyber space. This objective will be attained by improving the legal system, enhancing professional capabilities of law enforcement authorities while investigating criminal offences in cyber space, by developing analytical systems, implementing advanced methods and procedures of operation and technical tools intended to tackle criminal offences in cyber space.

22.2. *The second objective of the second target* is to strengthen prevention and control of criminal offences in cyber space. This objective will be fulfilled by advocating the society's self-defence culture and promoting responsible behaviour in cyber space, by improving the fulfilment of functions of law enforcement authorities in tackling criminal offences in cyber space and by ensuring more expedient international cooperation while investigating such criminal offices, developing effective cooperation of law enforcement authorities with educational institutions, representatives of private and public sector and the general public.

SECTION THREE
CYBER SECURITY CULTURE AND INNOVATION

23. **The third target of the Strategy** is to promote cyber security culture and development of innovation.

24. Cyber incidents are inevitable in the modern world. It is impossible to avoid them and be protected from them even if all existing cyber security measures are applied. For this reason, representatives of the public and private sectors must take care of improving their staffs' cyber culture. According to the data received from a survey carried out by IBM in 2017[6], the number of incidents which were caused due to negligence or ignorance of workers of the private sector which was surveyed (in 2017, the number of cyber incidents constituted more than 20%, in 2016 – 15%) has been increasing. More than 30% of such cyber incidents took place because workers opened the links or documents sent to them by offenders by email. In Lithuania, the number of emails created using social engineering methods has been also growing[7].

25. According to the summary data on the results of the implementation of European Innovation dated 2018, representatives of private sector in Europe have been increasingly focusing on the training of their staff members in the field of ICT, however, in Lithuania, this index slightly exceeds 10% (the average index in Europe is 21%). Public service employees in Lithuania are also provided with the opportunity to improve their skills in the field of cyber security. The number of civil servants who have taken cyber security course is annually growing (according to the data of the Civil Service Department, there were 146 such civil servants in

[6] IBM. *IBM X-Force Threat Intelligence Index 2018 (2018).*
[7] Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (2018). *2017 m. Nacionalinio kibernetinio saugumo būklės ataskaita*.

2015, 249 – in 2015 and 289 – in 2017). But regular training in cyber security for employees of the public and private sectors which could be organised taking into consideration the latest cyber security trends in Lithuania and in the world, would increase employees' vigilance, carefulness and cyber security culture.

26. To improve cyber security culture among the Lithuanian population continuous dissemination of information covering all relevant information on the latest cyber incidents and other actions that might pose threat to the security of personal data or make people the victims of criminal offences in cyber space must be ensured. According to the data of a special Eurobarometer survey 464a designed to identify the Europeans' attitude to cyber security, only 16% of the internet users in Lithuania think that the risk to become a victim of criminal offences in cyber space has not increased (the EU average – 11 %). Nevertheless, the extent of dissemination of this type of information should be greater since 46% of the internet users in Lithuania feel too little aware of the risks of criminal offences in cyber space (the EU average – 51%).

27. There have been a number of surveys and forecasts conducted in the world. Conclusions usually identify that people lack cyber security skills[8] and that this shortage will prevail in the future. The required competence may be ensured by quality education which meets labour market needs. Presently, cyber security programmes are offered by four universities in Lithuania, however, referring to the results of the survey carried out by the association Infobalt and a public institution Invest Lithuania titled "The ICT Specialists in Lithuania: Situation in the Labour Market and Employers' Needs", the existing situation fails to meet the needs of the labour market, for this reason, to reduce the gap between the demand and supply of cyber security specialists, the existing study programmes must be developed and strengthened and new study programmes aimed at training cyber security specialists must be created.

To achieve higher cyber security culture, it is important that children are taught the basics of cyber security according to pre-school and/or pre-primary general education programmes and schoolchildren – according to primary, basic and secondary education programmes since ICT is used on an increasingly wider scale to ensure educational and learning process.

To carry out reorganisation of teacher training and qualification improvement system as stipulated in the programme of the Government of the Republic of Lithuania, effort should be also put to improve teachers' qualification in the field of cyber security. Teachers of different education areas who have the opportunity to expand and deepen their competences in the field of cyber security will have "tools" to succeed in educating schoolchildren and students and in this way will contribute to the development of a knowledge and innovation based society as well as to the strengthening of cyber security.

28. Many cyber security experts[9] estimate that by the year 2019 there will be at least 1.5 million vacancies for cyber security specialists in the world. The study "ICT Specialists in

[8] ISACA. *State of Cybersecurity 2018 (2018),* Information Security Community on LinkedIn, (ISC)². *Cybersecurity Trends. 2017 Spotlight Report (2017).*
[9] Silensec. *Addressing the Cyber Security Skills Gap (2017).*

Lithuania: Situation in the Labour Market and Employers' Needs" conducted by the association Infobalt and public organisation Invest Lithuania in 2018 revealed that the number of ICT specialists in Lithuania amounted to 22,600 and that about 13,300 different ICT specialists would be needed within the following three years. Regrettably, researchers provided no details about the lack of cyber security specialists in Lithuania, however, an assumption may be made that cyber security specialists constitute a considerable number of specialists that are in high demand. To tackle the problem of the shortage of cyber security specialists, first, it should be identified, what type of cyber security specialists are most wanted since, based on the conclusions of studies carried out in other countries[10], different number of cyber security specialists might be needed in different countries, problems related to the lack of cyber security skills might differ; besides, specialists might be in demand only some areas of cyber security.

29. Rapid development of cyber space leads to emergence of opportunities to promote innovation which drives efficiency and economic growth: it prompts the creation of new and better jobs, increase in social mobility and entails a response to global social and security challenges.

Lithuania joined the European Union relatively not long ago; for this reason, there is no in-depth scientific research on cyber security or its teaching traditions. The latter have been well-established in in other EU Member States. Lithuania has a lot of possibilities to improve the use of the opportunity given by the EU to promote investment in scientific research, notably, to avail of the general research and innovation programme Horizon 2020 (2014–2020) and this way contribute to the strengthening of digital economy development and defence policy on the national as well as on the EU scale. The state's effort must be focused on different support measures which allow the representatives of private sector to get access to and affiliate with international networks when looking for potential employees and partners. This would stimulate the private sector to invest in the areas of scientific research, experimental development and innovation, create new products and services – in the cyber security area as well. The designing of innovative cyber security products would serve as an additional impetus and as a tool for boosting the competitiveness of Lithuania's industry. Besides, innovative cyber security products are necessary to resist modern cyber incidents. It is also important to promote the participation of Lithuania's researchers in organising international joint research publications in the field of cyber security, to attract as many students as possible, to participate directly in high level projects of experimental development focused on cyber security and, to expand cooperation of public and private sectors with science and education institutions, to increase the number of foreign doctoral students in the area of cyber security.

30. According to the data of the European Innovation Scoreboard 2018, to compare with other EU Member States, Lithuania is a moderate innovator; however, it has advanced considerably in terms of promotion of innovation and improvement of the ecosystem of

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

innovation[11]. In the European Union, private sector still allocates fewer funds to innovation than its rivals beyond the borders of the EU. No reliable measurements of the cyber security market have been carried out in Lithuania yet. Nevertheless, it is acknowledged that the market has been growing; for this reason, innovation would help coherently create and strengthen the status of Lithuania as of a competitive country which develops innovative cyber security products and services. This synergy may be attained by joining the initiatives of innovation with the general country's policy while seeking for a long-term science, technology and innovation development.

31. Lithuania has a regulatory and supervisory environment which is favourable to the activities of financial services and promotes innovation in the finance sector. Pursuant to the data of Lithuania Fintech Report 2017, in 2017, there were117 FinTech enterprises operating in Lithuania. This area is one of the strategic activity directions of the Bank of Lithuania, thus, its activity in one of the most promising and prospective financial technology innovation, namely, block chain technology, will effectively contribute to the development of FinTech innovation.

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

32.1. *The first objective of the third target* is to expand scientific research and activities which create high added value in the area of cyber security. This objective will be fulfilled by creating suitable conditions for the creation of new, advanced capabilities which develop cyber security initiatives by promoting the growth of the cyber security market, export of cyber security services to foreign markets, by expanding the cyber security sector of financial technology and by carrying out corresponding research.

32.2. *The second objective of the third target* is to develop creativity, advanced capabilities and cyber security skills and qualification which match with the needs of the market. This objective will be attained by having representatives of public and private sector as well as science and education institutions create a cyber security competence model, establish cyber security competence standards, develop systems of training, accreditation and certification all of which would be oriented towards the needs of the labour market, also have them attract and develop talents, create training and testing environment of cyber security, teach the beginners/newcomers and provide opportunities of re-training/re-qualification to persons working in the ICT field, improve knowledge on cyber security of persons who work with sensitive data.

32.3. *The third objective of the third target* is to promote the cooperation between the public and private sector and science and education institutions in developing cyber security innovation. This objective will be fulfilled by identifying the common needs of private and public sectors, their importance to scientific cyber security research, by creating technical measures, methods and other resources, by developing competences to resolve cyber security problems and carry out specific cyber security objectives.

SECTION FOUR

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

PUBLIC AND PRIVATE SECTOR COOPERATION

33. **The fourth target of the Strategy** is to strengthen a close cooperation between private and public sectors.

34. In modern states, in which broadband infrastructure is well developed, representatives of the public sector can no longer combat dangerous cyber incident or cyber incidents, which have a substantial impact, on their own. Managers of critical information infrastructure – often representatives of the private sector – are not always capable of containing cyber incidents, the extent of which exceeds their organisation's capacity all by themselves. Thus cooperation between public and private sectors becomes inevitable in order to ensure full cyber security. The main condition for cooperation between private and public sectors is a fully-fledged partnership which entails trust and benefit; for this reason, public and private sector cooperation should make an endeavour 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 cooperation between private and public sectors on a political level. All effort must be made to effectively enjoy the rights of a Cyber Security Council which are defined in the Law on Cyber Security.

36. To ensure cooperation between private and public sectors Cyber Security Information Network (hereinafter referred to as the "Network") is used. One of the purposes of the Network is to share information on potential and past cyber incidents as well as exchange recommendations, instructions, technical solutions and other measures which ensure cyber security and cooperation among the members of the Network in the field of cyber security. It is necessary to integrate measures in the Network which help ensure efficient and mutual trust so as to promote communication among the Network Members.

37. The ICT is used on a broad scale and its advantages in the 21st century is undoubtful, however, the prevalence of the ICT raises questions of how about respond to the identified ICT security loopholes in an effective manner. Gaps in the ICT security are searched for by the persons who have different goals; however, in order to develop a responsible approach for unveiling the gaps in the ICT security, it is important to create suitable conditions for a person, who has detected a gap and wants to remedy it, to cooperate with the cyber security entities whose ICT security loophole was disclosed. Having identified and publicly announced the procedure for disclosure of ICT security gaps, cyber security entities would thus be protected from possible damage caused by cyber incidents or would considerably diminish it. Establishment of the procedure for revelation of gaps in the ICT security and their public announcement would contribute to the assurance of the country's cyber security and would provide more opportunities for cooperation between private and public sectors.

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

38.1. *The first objective of the fourth target* is to improve the coordination of cooperation between private and public sectors. This objective will be reached by creating a sustainable model of cooperation between private and public sectors in the field of cyber security, by identifying responsibility and capabilities, by strengthening the country's cyber security, by making exchange of relevant information on cyber threats, cyber incidents which have taken place and lessons learned between private and public sectors more effective, by developing early warning system, by creating new and improving the existing communication methods and processes.

38.2. *The second objective of the fourth target* is to increase the degree of cyber security maturity of the representatives of private small and medium-sized businesses. This objective will be fulfilled by encouraging (urging) the representatives of small and medium-sized businesses to check the status of their cyber security and plug the gaps in cyber security.

38.3. *The third objective of the fourth target* is to create responsible practice of disclosing the ICT security gaps in private and public sectors. This objective will be reached by initiating a responsible practice of disclosing ICT gaps in private and public sectors, by establishing operational principles of this field, the procedure of application of methods, technical capacities and other measures designed for this purpose.

SECTION FIVE
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 cyber security.

40. Lithuania's national security and prosperity of its society is directly dependent on stable, easily and freely accessible and secure cyber space. Taking into consideration the fact that cyber threats and risks have become of cross-border nature and no longer respect but rather defy national borders, Lithuania will seek to strengthen its national cyber security by actively cooperating with bilateral and multilateral partners and by taking part in international forums designed for settlement of cyber security related problems and problems of managing the global virtual space in a targeted manner.

41. Lithuania aspires to become an active part of an international community which seeks to resolve cyber security and internet management problems, to actively cooperate with partners and allies by signing an international agreement on legal regulation of cyber space which shall be based on the compliance with the provisions of international law, provisions and principles applied to activities in this space, security of the open internet, and protection of human rights and freedoms in cyber space. Lithuania will put particularly much focus on the cooperation with NATO, the European Union and other countries which adhere to democratic principles in the field of cyber defence. Lithuania supports as close and sustainable cooperation with NATO and the European Union in the area as possible with the aim to avoid overlapping of functions and

activities. Lithuania will strengthen bilateral cooperation on political and technical levels with the United States of America, in particular.

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 and cooperation among the countries of the Baltic region in the field of cyber security. This objective will be fulfilled by taking part in the activities of the European Union, NATO, the United Nations, the Organisation for Security and Cooperation in Europe, organisations of the Baltic region and other international organisations.

42.2. The *second objective of the fifth target* is to strengthen international cyber security capabilities and capacities. This objective will be accomplished by initiating and managing a project of Permanent Structured Cooperation with the aim to consolidate cooperation in the field of cyber security and defence of those European Union Member States, the civil and military capabilities of which meet higher criteria and are tied by greater commitments.

42.3. *The third objective of the fifth target* is to further develop the dialogue with the United States in the field of cyber defence, to strive for the involvement of the US in Lithuania's cyber security assurance projects. This objective will be attained by developing bilateral cooperation between Lithuania and the US on political and technical scale and by pursuing activities which strengthen cyber defence and security of Lithuania in cooperation with the United States of America.

CHAPTER III
IMPLEMENTATION OF THE STRATEGY AND RESPONSIBILITY

43. To implement the targets and objectives of the Strategy, the Government of the Republic of Lithuania shall approve an interinstitutional operating plan which shall establish measures for the implementation of the Strategy and allocate the funds to this end. Drawing up of this plan shall be coordinated by the Ministry of National Defence with participation of the NCSC. Ministries, other state and/or municipal authorities, agencies and/or organisations specified in the interinstitutional operating plan of the Strategy shall participate in the implementation of the Strategy within their competence (hereinafter referred to as the "Strategy Executors").

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

45. The Strategy shall be implemented using the allocations of the Republic of Lithuania state budget planned for the respective year, also the funds of municipal budgets, support of the European Union and other international financial support, and other legally obtained funds. The responsibility for the planning of the required financial resources, which shall be carried out on the basis of the principle of subsidiarity as is entrenched in the Law on Cyber Defence, shall be assumed by the Strategy Executors.

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 based on the use of publicly available data of sociological opinion polls and surveys conducted by the Lithuanian Department of Statistics and Eurostat. Monitoring of the results of the Strategy's implementation will be conducted by the Ministry of National Defence, the NCSC and Cyber Security Council.

47. The Strategy Executors shall provide the NCSC with information on the course of the implementation of the Strategy, its effectiveness and the supporting documents at the end of a year, no later than before 15 January of the following year. This information may be accompanied by the suggestions/proposals for specification of the Strategy and/or implementation documents. At the request of the NCSC, the Strategy Executors must furnish any other information required for the monitoring of the results of the Strategy implementation. All stakeholders are entitled to put forward proposals regarding the update of the provisions of the Strategy at any time during the period of the Strategy's implementation.

48. After the receipt of information specified in Paragraph 47 of the Strategy, the NCSC shall provide the Ministry of National Defence with the systematised data on the state of implementation of the Strategy's targets and objectives of the previous year and shall also forward the suggestions and indicate the 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 received information on the previous year and the data on the course of implementation of the Strategy and efficiency every year before 1 March. The systematised data on the annual implementation of the Strategy shall be then 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 in relation to the annual and final assessment of the implementation of the Strategy shall be announced on the website of the NCSC.

51. The NCSC shall draft a final assessment of the implementation of the Strategy six months before the deadline for the implementation of the Strategy 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 THE ASSESSMENT OF IMPLEMENTATION OF THE NATIONAL CYBER SECURITY STRATEGY AND THE LIST OF TARGETED VALUES

Item No.	Name of evaluation criterion	Value of the evaluation criterion			Agency or body which carries out monitoring of the achievement of the evaluation criterion
		Initial value in 2017	2021	2023	
The main target of the National Cyber Security Strategy (hereinafter referred to as the "Strategy") is to provide the Lithuanian society with the opportunity to exploit the potential of information and communications technology (ICT) by identifying cyber incidents in an effective and timely manner, preventing their occurrence and spread, and managing consequences resulting from cyber incidents.					
	Position of the Republic of Lithuania in the global cyber security index rating 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 is to strengthen cyber security of the country and the development of cyber defence capabilities.					
2.	Percentage of cyber security entities (agents) which meet cyber security requirements (not lower than specified)	*	35	50	Ministry of National Defence
3.	Percentage of public sector websites which 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 which participate in national cyber security exercises/trainings (not lower than specified)	42	60	70	Ministry of National Defence
5.	Percentage of modernised cyber security and cyber defence capabilities of the state (it shall be not lower than specified)	Restricted (R)	R	R	Ministry of National Defence
The second target of the Strategy is to ensure prevention and investigation of criminal offences in cyber space.					

Item No.	Name of evaluation criterion	Value of the evaluation criterion			Agency or body which carries out monitoring of the achievement of the evaluation criterion
		Initial value in 2017	2021	2023	
6.	Percentage of officers who have completed training, public prosecutors, specialists, experts involved in investigation of criminal offences in cyber space (not lower than specified)	*	70	90	Ministry of National Defence in cooperation with the Strategy Executors
7.	Number of developed or implemented technical tools, procedures, analytical platforms designed for dealing with criminal activities in cyber space (in units), not lower than specified	*	2	5	Ministry of National Defence in cooperation with the Strategy Executors
8.	Number of projects intended for the prevention and control of criminal offences in cyber space (in units), not lower than specified	2	2	2	Ministry of National Defence in cooperation with the Strategy Executors
9.	Number of participations in international events and working groups meant for the prevention and investigation of criminal offences in cyber space (in units), not lower than specified	12	14	15	Ministry of National Defence in cooperation with the Strategy Executors
10.	Number of participations in international operations while investigating criminal activities in cyber space (in units), not lower than specified	3	4	6	Ministry of National Defence in cooperation with the Strategy Executors
The third target of the Strategy is to promote cyber security culture and development of innovation.					
11.	Total number of projects, which promote the development of innovation in the sphere of cyber security, since 2018	0	5	10	Ministry of National Defence in cooperation with the Strategy Executors
12.	Amount of investments in the promotion of digital literacy culture, development of knowledge on security and scientific research	*	1, 000	2, 000	Ministry of National Defence in

Item No.	Name of evaluation criterion	Value of the evaluation criterion			Agency or body which carries out monitoring of the achievement of the evaluation criterion
		Initial value in 2017	2021	2023	
	(Eur, thousand), not lower than specified				cooperation with the Strategy Executors
13.	Number of persons who have obtained qualification in cyber security (in units), not lower than specified	33	200	400	Ministry of National Defence in cooperation with the Strategy Executors
14.	Percentage of public service employees and employees of public authorities and institutions working under employment contracts 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 Executors
The fourth target of the Strategy is to strengthen a close cooperation between private and public sectors					
15.	Number of models developed through cooperation of public and private sectors in the field of cyber security, in units	0	0	1	Ministry of National Defence in cooperation with the Strategy Executors
16.	Percentage of managers of state information resources and of critical information infrastructure incorporated in the cyber security information network, not lower than specified	36	86	90	Ministry of National Defence
17.	Number of measures designed for the improvement of the cyber security state of representatives of public and private (small and medium-size enterprises) sectors (in units), not smaller than specified	0	4	6	Ministry of National Defence in cooperation with the Strategy Executors
18.	Number of measures designed for the formation of practice of disclosure of gaps in the ICT security of public and private sectors (in units), not smaller than specified	0	1	2	Ministry of National Defence in cooperation with the Strategy Executors

Item No.	Name of evaluation criterion	Value of the evaluation criterion			Agency or body which carries out monitoring of the achievement of the evaluation criterion
		Initial 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 cyber security.					
19.	Percentage of participation in the meetings, forums or other events on the 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 Executors
20.	Percentage of participation in the meetings of working groups of international organisations for investigation of cyber incidents 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, EU Member States, NATO Member States, countries of the Baltic region and other countries in the field of cyber defence (in units), not smaller than specified	2	1	2	Ministry of National Defence in cooperation with the Strategy Executors

* 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.

_____