University of Salford A Greater Manchester University
University of Essex ESSEX BUSINESS SCHOOL International Centre for Entrepreneurship Research
The General Jonas Žemaitis Military Academy of Lithuania
Ministry of National Defence Republic of Lithuania
Vilnius Gediminas Technical University
RISEBA
Estonian Business School
NATO Energy Security Centre of Excellence
ENTREPRENEURSHIP AND SUSTAINABILITY CENTER
AVADA

JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2017 March Volume 6 Number 3
http://dx.doi.org/10.9770/jssi.2017.6.3(3)

A MODEL FOR THE NATIONAL CYBER SECURITY STRATEGY. THE LITHUANIAN CASE

Darius Štitilis[1], Paulius Pakutinskas[2], Marius Laurinaitis[3], Inga Malinauskaitė-van de Castel[4]

[1,2,3,4] Mykolas Romeris university, Ateities 20 LT-08303, Vilnius, Lithuania

E-mails: [1]stitilis@mruni.eu; [2] paulius.pakutinskas@mruni.eu; [3]laurinaitis@mruni.eu; [4]inga.malinauskaite@mruni.eu

Received 19 June 2016; accepted 18 December 2016

Abstract. Given the global nature of cyber threats, assurance of a cyber security policy is very important not only at the local organisation level, but also at national and international level. Currently, cyber security as such is not suitably regulated internationally; therefore, the role of national cyber security strategies has become particularly significant. Lithuania is among the leaders in the EU and globally in the development of the optical fibre network. FTTP coverage has already reached 95%, the highest in the EU. Regardless of that, the cyber security programme effective in Lithuania does not provide conditions to ensure an appropriate level of cyber security and may not be regarded as a high-level contemporary strategic document in the area of cyber security. This article presents a study the main outcome of which are guidelines for a contemporary model of the Lithuanian national cyber security strategy. Based on comparative and historical studies as well as expert interviews conducted by authors and on the best practice of other countries, the article presents the elements of a model of the Lithuanian national cyber security strategy as well as guidelines on the content of these elements of the model. The article also reveals which elements of the model of the national cyber security strategy should most of all reflect the national situation and which elements may be unified and possibly also adapted in the cyber security strategies of other countries.

Keywords: cyber security, strategy, model, regulation, Lithuanian case study

Reference to this paper should be made as follows: Štitilis D.; Pakutinskas, P.; Laurinaitis, M.; Malinauskaitė-van de Castel, I. 2017. A model for the national cyber security strategy. The Lithuanian case, *Journal of Security and Sustainability Issues* 6(3): 357–372. http://dx.doi.org/10.9770/jssi.2017.6.3(3)

JEL Classification: O33; D80

1. Introduction

Nations have become dependent on their information and communications infrastructure and threats against its availability, integrity and confidentiality can affect the very functioning of our societies (Klimburg, A. 2012). The importance of cyber security, as a new category additionally stressing cyber threats from the internet, is increasing. Cyber security is even described as "the cornerstone of the information society" (Schjolberg S. and Ghernaouti-Hele S., 2011). Cyber security requires coherent and detailed strategic planning, appropriate legal regulation and other related measures. Recently, countries all over the world have been increasingly focusing on the drawing up of new laws and other documents as well as the adoption or update of national cyber security strategies. According to research, currently, the majority of countries have the approved and effective national cyber security strategies. The adoption of cyber security strategies has been particularly on the rise as from 2011. It is during this time that many European Union member states and countries from around the world adopted cyber security strategies (Cyber security strategies, ENISA). Thus the adoption of national cyber security strategies has been especially active in the recent years. Certain countries already adopted a second version of such a strategy (Estonia, the Netherlands, the Czech Republic, etc.). Countries have made great progress in developing and implementing their strategies (Good Practice Guide, 2016). For example, the second strategies focus on strategies and re-

finement of institutional responsibilities, strategies talk about the development of abilities in the cyber security area, enclose specific action plans in the cyber security field (Štitilis, D et al. 2016a).

However, regardless of such a high level of activity, national cyber security strategies of individual countries differ in their content, their form, their implementation and other elements. There is currently no unified national framework for improving cybersecurity (Fisher E.A. 2009). Internationally, the area of cyber security is practically not coordinated at all[1], while the EU adopted a Cyber Security Strategy in 2013 and the *Directive* on *Security of Network and Information* Systems in 2016. The EU Cyber Security Strategy provides general guidelines for ensuring cyber security in the EU, while the directive introduces an obligation for every EU member state to have an approved national cyber security strategy and specifies the questions to be covered by such a strategy. However, the directive will have to be implemented only as from 9 May 2018. Besides, the directive provides only abstract information on the elements of a national cyber security strategy.

A contemporary model of the cyber security strategy can help each country to focus on the key and essential questions of improvement and assurance of cyber security and resistance. A contemporary cyber security strategy can do more than just have a positive impact on the assurance of cyber security in a country. The existence and proper implementation of such a strategy can help address national security and other relevant questions of an appropriate country as well as ensure proper development of a modern society. Secretary General of NATO Jens Stoltenberg has stated that "cyber is now a central part of virtually all crises and conflicts" (NATO Chief: Cyber Can Trigger Article 5). Thus an efficient national cyber security strategy can even help resolve conflicts between countries and ensure peace. However, each country has its own national specific features and that could also possibly determine the content of a national cyber security strategy. Yet, on the other hand, the national specific features should not hinder efficient international cooperation, exchange of best practice or operational-level assistance and appropriate defence.

Methodology. In preparing this paper and presenting the outcomes of research (guidelines), the authors used several methods, including a comparative analysis of cyber security strategies which enabled them to thoroughly examine and compare the provisions of the strategies; a historical analysis of the provisions of national cyber security strategies which enabled them to make assumptions and record observations in the historical context of strategy development, and other methods. A qualitative research was also carried out since a more profound analysis of the phenomenon required specific knowledge and experience of respondents. To analyse the models of cyber security strategies the best decision is to expert knowledge by employing the method of surveying experts' opinions as this helps accumulate the latest scientific knowledge. In this particular case, the authors interviewed experts of two specific levels i.e. they submitted their questionnaires to foreign and national experts asking them to complete the questionnaires in writing (in national expert`s case – semi-structured interview). The research results were also validates through three different types of activities, including validation during international scientific conference.

Thus, in order to present the guidelines for a model of the Lithuanian national cyber security strategy, the authors conducted a survey of international cyber security experts. The authors also used the results of a comparative study of the strategies of EU and NATO countries (which partially overlap), the results of a historical study of certain selected EU and NATO countries, the results of the analysis of the content of cyber security strategies of EU and NATO countries as well as the results of a survey of Lithuanian cyber security experts. Overall, used methodology may be presented below.

[1] In 2002, OECD adopted the Information Security Guidelines the principles of which passed a test of time, but still, this document may not be applied taking into account contemporary relevant issues of cyber security and contemporary cyber security risks.

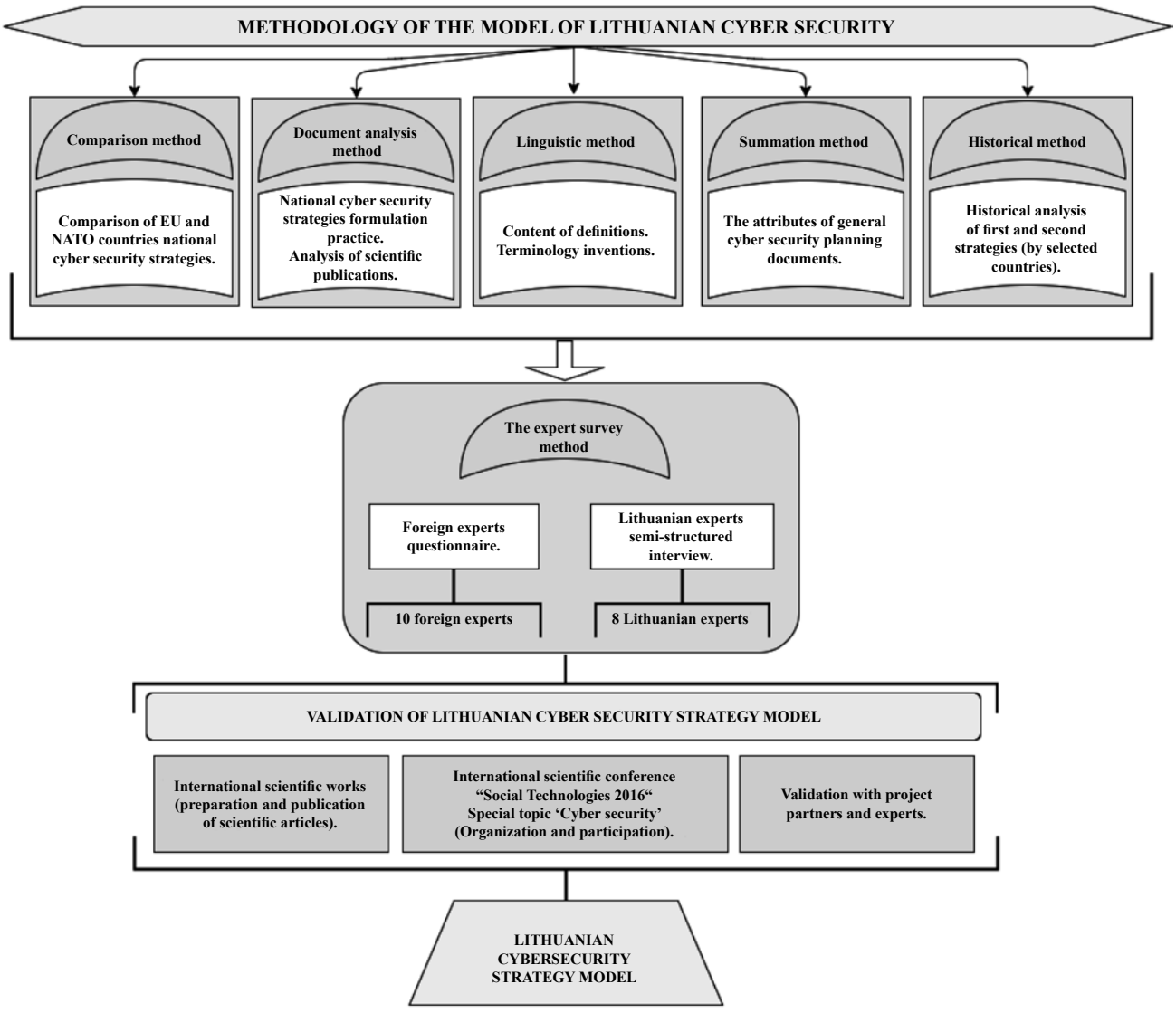

Fig.1. Methodology.

Source: Designed by the authors

2. Overview of the national cyber security situation in Lithuania

1.1. Specific features of technologies.

For the purposes of the national cyber security situation, the level of development of electronic communications networks and of technologies of an appropriate country is crucial. In terms of internet coverage, Lithuania takes the 7th place out of the 28 EU member states (European Union data). In the Republic of Lithuania, modern technologies are especially prevalent, in particular the EDGE technology, the development of the 4G mobile network and the Wimax 4G internet. Besides, Lithuania has one of the best indicators in Europe of the services of the NGA (Next Generation Access). FTTP coverage has already reached 95%, the highest in the EU. Lithuanian consumers also benefit from the most affordable broadband in Europe, when compared to their income: an average EU consumer has to spend almost twice as much of their income on broadband than Lithuanian residents. According to the official data of the Department of Statistics of the Republic of Lithuania, in 2016, 100% of companies used computers in their activities, 100% of companies had internet access, and 77% of companies had their own websites (The official statistics portal, Lithuania). In terms of the use of e-government services, i.e. the submission by residents of various completed electronic forms to state institutions, in 2015, Lithuania took the 8th place in the European Union.

1.2. Usage of electronic services

The statistics show that the residents of Lithuania use e-services increasingly more often:

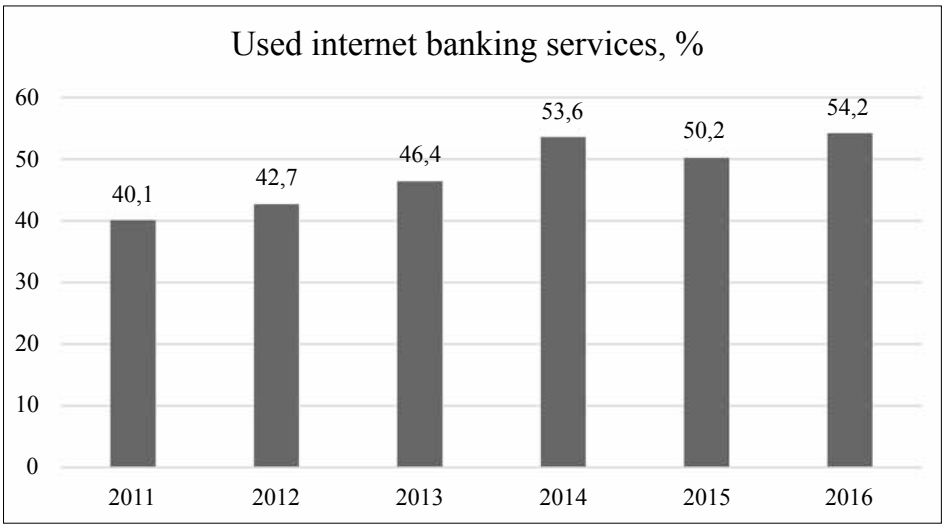

Fig.2. Use of online banking services.

Source: Designed by the authors.

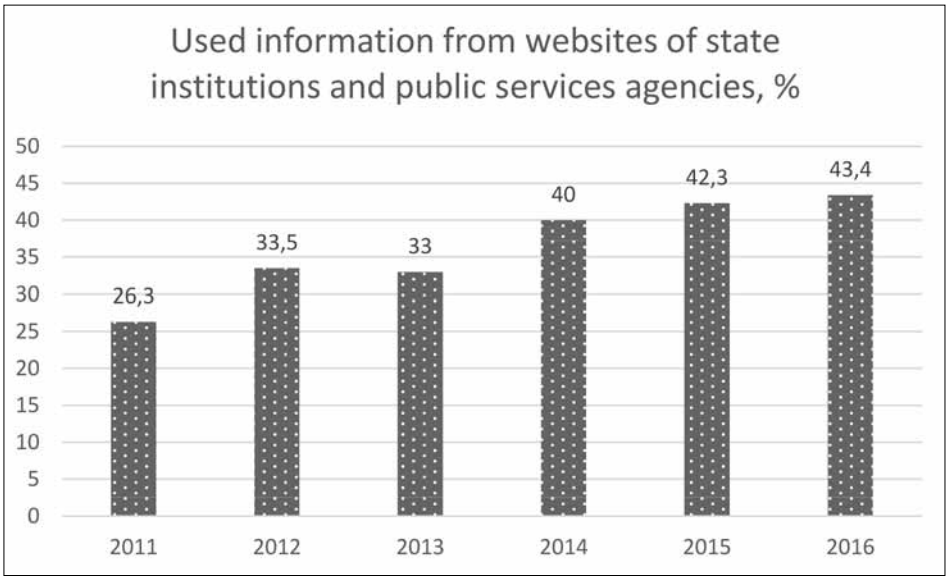

Fig.3. Use of information from websites of public institutions.

Source: Designed by the authors.

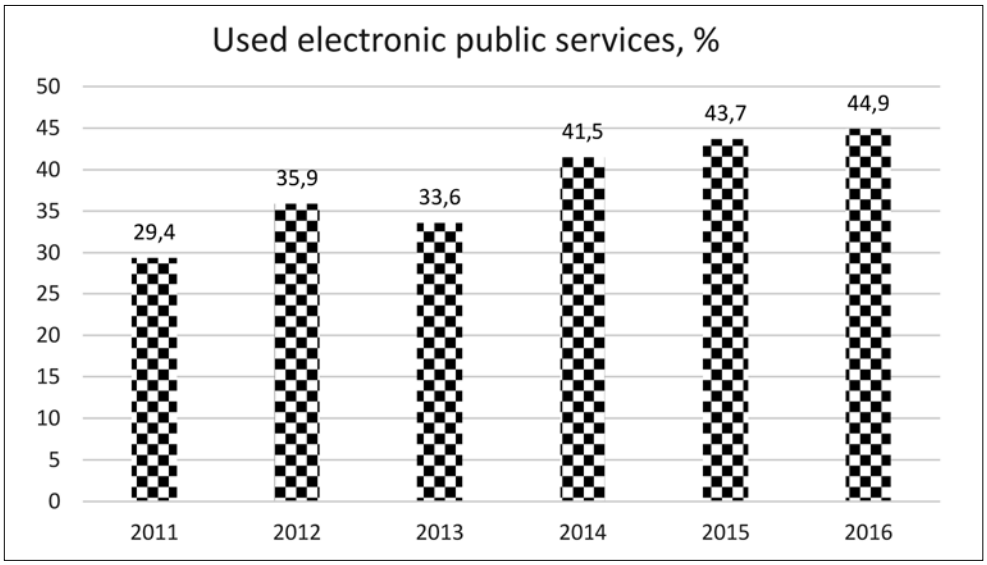

Fig.4. Use of electronic public services.

Source: Designed by the authors.

The statistical indicators mentioned above and related information make it possible to maintain that the analysis of the current situation of cyber security in Lithuania as well as generalisations with regard to the legal environment in the area of cyber security and problems raised may serve as a good example for other countries. It is noteworthy that the population of Lithuania stands at 2.92 million (2016), while its area is equal to 65.300 sq. meters. The capital is Vilnius, with the population of 540.608. In the Republic of Lithuania, there are 2.399.678 internet users, i.e. 84.1% (on 31 December 2014). More data on electronic communication services and market in reports of Communications Regulatory Authority of the Republic of Lithuania.

1.3. The geopolitical context and situation related to cyber incidents.

It is advisable to discuss the geopolitical context of Lithuania, as a state, as much as this is related to cyber security. The geopolitical context may reveal external threats to the country itself, and that should be reflected in the cyber defence policies of an appropriate country. According to the State Security Department and the Ministry of National Defence (Assessment of threats to national security), in 2015, the security situation in Lithuania's neighbourhood and in the entire Eastern European region remained tense. With regard to Lithuania, negative cyber activities of Russia and its negative foreign policy was increasing. The significance of military power for the general security situation in Eastern Europe and the security of concrete countries, which had increased a lot in 2014– 2015 due to Russia's actions in Ukraine, remained high. Deployment of Russia's military capabilities in Lithuania's neighbourhood and deployment of NATO forces in Lithuania, on the other hand, show that Lithuania finds itself on the spearhead of interests and that the situation in Lithuania and Lithuania's neighbourhood is heated. Besides, in 2015, the question of the security situation in Eastern Europe started to be overshadowed by the fight with terrorism and the migration crisis. These questions are also among the most important ones on the agenda of the European Union (hereinafter referred to as "The EU"), NATO and many countries in 2016.

The situation related to cyber incidents and their number is constantly on the increase. According to the data of CERT-LT for Quarter II of 2016 (Operational report of CERT-LT for Quarter II of 2016), the number of cases of overtaking of information systems (2,290) and forgery of electronic data (147) has been growing for several quarters now: Te number of incidents of both types was almost 80 per cent higher than a year ago. Besides, the number of cases of disruption of electronic services has increased significantly and stands at 36. In April and May of the quarter in question, continuous Distributed Denial of Service (DDoS) attacks took place, as directed against the websites of institutions of the Republic of Lithuania, the media, banks and the private sector. During these attacks, ill-willed persons used various methods of attacks, aggravating the defence of website adminis-

trators and the management of these attacks. According to CERT-LT, the recent cyber attacks are complex and differ according to the methods used.

According to the same study, cyber espionage, attacks (DDoS attacks, changes to user interfaces, etc.), cyber intelligence (scanning) were the activities most frequently recorded in the cyber space in 2015, as directed against state institutions of Lithuania, objects having a strategic significance to the country's national security and the private sector. In 2015, it was noticed that financially-motivated cyber hackers sought not only economic but also political benefit. In 2015, yet another trend was established when real developers and distributors of the malicious code increasingly more often used various means and resources to mask themselves and hide, i.e. to remain unidentified or mistakenly identified: "stolen signatures" were inserted into the source code, which were parts of the source code hiding the real purpose of the malicious code. Thus, considering both the financial and political context, cyber espionage against the state institutions of Lithuania, objects of the critical infrastructure of the country and the private sector remains one of the main threats to the country's national security. According to the study which was conducted, the companies causing highest danger to the Republic of Lithuania which were identified in 2015 are linked to Russia, China, India and Iran. Signs of the cyber weapon have been detected both in the networks and systems of the state institutions of Lithuania and objects of critical infrastructure of the country and in the terminal equipment of the private sector. The highest threat to the country's national security has been caused, as in recent years, by cyber hackers related to Russia, including Russia's intelligence and security services.

1.4. The general data about Lithuania

In 2015, Lithuania's gross domestic product comprised 41.2 billion US dollars (World Bank, 2016). Compared to 1995, when Lithuania's gross domestic product stood at 7.9 billion US dollars, an essential increase in the gross domestic product is observed. At the end of 2016, the population of Lithuania constituted 2.85 billion. It is noteworthy that the population of Lithuania is consistently a little decreasing due to emigration. Recently, Lithuanian public authorities have been initiating measures to stop the existing emigration and return a part of the emigrants from abroad, which should improve the demographic situation in Lithuania. Thus even though Lithuania is a country which is developing and modern, it is still quite small. It is believed that the Lithuanian national context of the cyber security situation should be taken into consideration in the preparation of Lithuanian strategic planning documents in the area of cyber security.

3. The historical context of cyber security strategic documents in Lithuania and the current situation

The need for strategic documents of a certain area emerged in Lithuania back in 2001 following the adoption by the Government of the Republic of Lithuania on 22 December 2001 of Resolution No 1625 "Regarding the approval of a state strategy of information technology security and its implementation plan". By this Resolution, the first national information technology security strategy was approved, however, the term "cyber security" was not yet used at the time. The main objective of this strategy was to regulate only the security of state institutions and agencies, while the security of information technologies of the private sector was not discussed therein. Bearing in mind that the major part of the infrastructure in Lithuania is managed by the private sector and from the point of view of current regulation, it is possible to maintain that the private sector should have been included into the strategic planning of cyber security at that time. This was done, but much later.

The second strategy – the National Strategy for the Security of Electronic Information in the Information Systems of Public Institutions – was approved in 2006 and remained in force until 2008[2]. The Strategy already uses a different term – "security of electronic information". However, this Strategy was also limited to the public sector. The main objectives of the Strategy included:
- To improve coordination and supervision of the security of electronic information;
- To regulate the security of electronic information by legal acts;

[2] However, this strategy was limited to the sector of public institutions.

- To improve the culture of the security of electronic information;
- To improve the security of the infrastructure for the transmission of electronic information; to promote the implementation of projects ensuring the security of electronic information.

This Strategy, like the one in 2001, appointed institutions responsible for the implementation of the Strategy. Compared to the previous strategy, the institutional model is applied much more widely, and as many as seven institutions were appointed as responsible for the implementation of the measures provided for in the Strategy of 2006, however, once again – only in the public sector. Besides, the functions of institutions were not clearly separated, in particular, in the context of policy formation and implementation – the responsible institutions were indicated only as responsible enforcers of the plan of measures. The main institution of Lithuania responsible for the security of electronic information was not identified either. The said state Strategy lost effect in 2008, and since then Lithuania has not had any effective strategy or programme for the security of electronic information.

The currently effective Programme for the Development of Electronic Information Security (Cyber Security) for 2011–2019 was approved in 2011 (Government of the Republic of Lithuania, Resolution No 796). This Lithuanian Programme outlines the main problems of electronic information security (cyber security), determines the objectives and tasks for the development of electronic information security (cyber security). The objectives and tasks set out in this Programme are focused on both the public and private sectors. Thus this Programme constitutes quite a major step forward. Regardless of that, we may mention the following shortcomings of the Programme:

- The objectives and tasks of the Programme are not concrete enough (abstract), and they do not reflect the dangers and risks of electronic space in all cases;
- To achieve the objectives and tasks, a system for the coordination of management of cyber security has not been created and allocation of concrete funds has not been provided for;
- The established indicators of the assessment criteria are specific and ambitious, but it is not clear how realistic they are, because most of the indicators have not been assessed at all until the adoption of the Lithuanian Programme, for example, the Programme provides that, by the year 2015, the level of information resources using the secure infrastructure will reach 70 per cent, and by 2019 – 100 per cent, although it is not known what this indicator was in 2011;
- The Lithuanian Programme does not distinguish the competences of any particular institutions in the field of cyber security, and only indicates the specific Lithuanian institutions and the specific objectives and tasks established in the Programme for the implementation of which they are responsible.

To compare this Programme with cyber security strategies of other countries, the authors performed a comparative study of cyber security strategies of EU and NATO states. A comparison of national cyber security strategies of EU and NATO countries was conducted by comparing the main criteria in the latest valid cyber security strategies of the respective countries:

1) principles,
2) cooperation with the private sector,
3) the fight against cybercrime,
4) cyber defence,
5) research,
6) standards,
7) support of fundamental values,
8) tasks and competence of “players”/authorities.

The concrete criteria were selected by assessing similarities and priorities of cyber security documents of the EU and NATO organisations. In the evaluation of the content of the cyber security strategy of an appropriate country, each criterion was assessed separately. The study resulted in various findings. Certain countries met all the selected criteria or did not satisfy just one criterion (for instance, the USA, Spain, the Czech Republic). Conformity of other countries with the selected criteria was diverse, conformity figures are quite different.

However, one country, namely Lithuania, stood out among others. The Lithuanian Cyber Security Programme did not comply with any criteria, except one – support of fundamental values. Thus the findings of the study have shown that the Lithuanian Cyber Security Programme, which should remain in effect even until 2019, does not conform to the provisions of strategic documents in the area of cyber security of the EU and NATO organisations most of all the EU and NATO countries.

The shortcomings of the Lithuanian Programme have also been, in fact, confirmed by the results of a survey of Lithuanian experts conducted by the authors. Thus even though Lithuanian strategic documents on cyber security so far are to be regarded as a step forward, Lithuania needs a new contemporary cyber security strategy which would be in conformity with the strategic objectives of the EU and NATO in the area of cyber security as well as would reflect real cyber security threats and the geopolitical situation of Lithuania.

4. Guidelines for a contemporary model of the Lithuanian national cyber security strategy

According to ENISA NCSS Good practice Guide, national cyber security strategies are the main documents of nation states to set strategic principles, guidelines, and objectives and in some cases specific measures in order to mitigate risk associated with cyber security. Following a high-level top-down approach, national cybersecurity strategy set the strategic direction for subsequent actions (Good Practice Guide, 2016). In this section, the discussion of the guidelines for a model of the Lithuanian national cyber security strategy will not include those possible parts of the model which, though important, are not to be regarded as essential. For instance, a preface, an introduction (which should present introductory aspects), executive summaries or a glossary. Hereinafter, the focus will be on the most important elements of a possible model.

According to the authors, like for any cyber security strategy, an overview of the national situation, including the cyber security situation, should be important. Such an overview would enable an understanding of a real situation in the country and, based on the presented analysis, would possibly adapt other parts of the strategy according to the national specific features. This is crucial because transplanting security threats that appear in other strategies but are not germane to the country formulating the strategy may do more harm than good by diverting national resources (Klimburg, A. 2012). Only the knowledge of the national situation makes it possible to formulate objectives, priorities, main areas of operation and other important parts of the strategy. As a national state, Lithuania has its own specific features as indicated above. It is also noteworthy that contemporary threats converge and, in addition to direct links to cyber security, threats may be related to weapons of mass destruction, terrorism, state failure and organised crime (Klimburg, A. 2012).

The overview of the national situation must discuss the legal environment of cyber security. Since a cyber security strategy is a planning document, which may also set plans at the level of legal acts, it is vital to review the legal environment of a national state. In addition to the Lithuanian strategic documents in the area of cyber security mentioned above in this article, in 2015, Lithuania adopted a law on cyber security which is to be regarded as the main legal act in the area of cyber security in Lithuania. However, one must bear in mind that, besides this document, other legal acts are also important for the Lithuanian legal system in terms of cyber security. For instance, the Law on the Fundamentals of National Security and the National Security Strategy establishing the fundamentals of national security. It is noteworthy that, in Lithuania, cyber security has already been integrated into national security. In addition, the Law on Information Resources of the State establishing the aspects of security of state information resources. Thus such national specific features of the cyber security situation should be discussed in a national cyber security overview.

Following an examination of the national situation, the model of the strategy should consistently move towards the principles. The problem of cyber security includes many areas of human activity and emerges from a technological change, i.e. technologies enabled the emergence of the security problems under discussion, however, problems are caused not by technologies but by people who use technological possibilities and adapt them for their purposes, i.e. the major part of the problems is not technological in nature but linked to the relationship of a human being with technologies and relationships of people with other people (for instance, systems are

disrupted on purpose not by technologies, even though accidental disruptions also take place due to imperfect technologies, but by people seeking selfish objectives (money, power, influence, etc.), i.e. the major part of issues are social and are studied by social sciences, therefore, these issues are resolved by applying the principles of social sciences, such as the principles of law, management, economics and others.

When establishing the principles in a strategy, it is advisable to establish special principles of cyber security strategies or principles which, in the context of cyber security, acquire higher importance than in other areas of human activity (Štitilis, D. et al. 2016b). However, it is crucial that the general or the special principles included in the strategy would indeed be key in order to ensure cyber security, then, having identified them in one document, we have a consistent system of principles, because principles are applied in the right manner only in a uniform system, while regarding one or another principle as absolute or too important may cause damage to the entire system and distort it.

Many discussions of cybersecurity include statements or lists of principles, which can be thought of as generally accepted characteristics or expectations (Fisher E.A. 2009). Based on studies conducted by the authors, it is recommended to indicate the following **principles** in a model of the Lithuanian cyber security strategy:

- Protection of fundamental rights (rule of law, subsidiarity, self-regulation, protection of personal data, proportionality, etc.). Cyber security is just one of the means to ensure fundamental human rights, therefore, this area of security may not become more important than the very human rights. When principles are applied, their systemic application is necessary, therefore, when applying the specific principles of cyber security, it is necessary to continuously take into consideration fundamental human rights as well as the principles of protection of privacy and communication and other principles.
- The principle of cyber security as an integral part of national security. This principle is necessary in order to ensure the importance and place of cyber security among other priorities of the state.
- The principle of cooperation including that of the public and private sectors (and the tertiary sector). This principle is important taking into account the specific features of a cyber network, i.e. for this network, geographic territories, borders of national states or departmental jurisdiction are not important, therefore, in order to achieve positive results it is necessary to strengthen all links, because the security of the system is worth as much as the weakest link of the system is worth. In the context of external and internal cooperation, all cooperating links are interdependent, therefore, they must coordinate their interests.
- The principle of personal responsibility. This principle indicates that cyber security, for the major part, depends on actions of individuals in using the cyber space and its means.
- The principle of proportionality. Thanks to this principle, means, resources and arising or potential risks must be appreciated. As quite a small country, Lithuania should not just copy the experience of the big countries in the area of cyber security – Lithuania should use the available resources for ensuring cyber security as efficiently as possible, taking into account concrete national possibilities of Lithuania.
- The principle of promotion of innovation, research and development. This principle is necessary taking into consideration the technological nature of cyber security. To ensure cyber security, the most advanced technologies should be implemented and the most recent threats should be responded to. Also innovation and research in the 21st century are increasingly becoming international endeavours (Olaniyi, E. O.; Reidolf, M. 2015).
- The principles of comprehensiveness, integrity, proactivity and solidarity are important seeking to assess the comprehensive nature of cyber security and apply the most efficient means. These principles are of the comprehensive nature and are characterised by the remaining basic elements which are necessary for every modern national cyber security strategy. Lithuania is no exception.

While the overarching goal of achieving comprehensive security remains (and some might argue is promoted), this development acknowledges that achieving a 100% protection level is neither feasible not realistic. Thus the need to identify new defensive and mitigating measures to provide security (Klimburg, A. 2012).

Taking into account the Lithuanian context, the following cyber security goals, areas of operation and priorities are to be provided for:

Table 1. Goals, areas of operation and priorities.

Goals of a cyber security strategy:						
• To ensure, for five years, appropriate and timely prevention of possible threats to the electronic space in Lithuania. • To increase, gradually, the number of responsible controlling forces by increasing information of consumers and their confidence in the electronic space in a targeted manner. • To provide for a centralised and proactive cyber defence plan including different state segments and levels.						
Main areas of operation						
Protection of critical infrastructure	Protection of state information resources	Cooperation of the private and public sectors	Formation of the institutional system	Development of the cyber culture	International cooperation	Development of the legal environment
Priorities:						
To ensure provision of important information services. A centralised decision-making and management system of holders of the critical infrastructure. Definition of methods of protection of the critical infrastructure. Collection, transfer and use of the best practice of other countries in the Republic of Lithuania. Search for financing for technical solutions of the critical infrastructure. Training for the staff responsible for the critical infrastructure.	To ensure protection of state information resources. To ensure implementation of advanced security solutions. Installation of organisational and technical protection measures. Search for financing for the said measures. Formation of the best practice is underway. Attraction of cyber security specialists.	To ensure appropriate competence of newly trained specialists and form the necessary skills. To ensure cooperation with the private sector. To ensure management of cyber threats in the public and private sectors. To ensure general operation of a national supervision and monitoring system. Development of possibilities to expand the existing structure of cooperation of the private and public sectors. Development of possibilities for innovative small cyber security business to receive financing easier. Strengthening and streamlining of cooperation on cyber security in various sectors of economy, including training and education in the area of cyber security.	To ensure functioning of notifications on violations of law in the electronic space. Establishment of one main institution responsible for cyber security in Lithuania. Review of the functions assigned to the existing institutions and their adjustment on the basis of need.	To ensure formation of cyber security policies taking into account international experience. To ensure education of consumers of information services. Increase of cyber security awareness and practical sessions. Preparation of courses on cyber security for schools and universities and introduction of programmes.	To ensure international cooperation seeking protection of particularly important information infrastructure. To ensure international cooperation for the fight with violations of law in the electronic space. To ensure cooperation with allies and partners. Establishment of a cyber security cooperation group of the Baltic States (if such group is non-existent).	To ensure functioning of a legal system in the area of cyber security. To combine institutes of security of electronic information and cyber security and appropriately draw up necessary amendments to legal acts. To unify definitions in the entire legal regulation. To examine compatibility and relevance of legal acts necessary for the implementation of the Law on Cyber Security. To implement appropriate and necessary changes in regulation.

Source: Designed by the authors.

Strategies are usually less explicit when it comes to how the government may address identified threats and challenges, including resources that may be necessary or questions about which departments should take the lead in response (Catherine Dale, 2008). This is not altogether surprising since a NSS usually serves to provide strategic guidance to government ministries and agencies (Klimburg, A. 2012). Therefore, while formulating guidelines, the authors did not try to provide for in detail as to how specifically the objectives and tasks of the strategy should be implemented and which concrete institutions should do that.

As indicated in the National Cybersecurity Framework Manual, "A national cybersecurity strategy should not exist in a strategic vacuum. On the contrary, it should be linked to existing national and international strategies to the extent that it is feasible to encourage a harmonised set of policies that are shared with likeminded partners. The linking of a NSS with other strategies may also be helpful to promote coordination, cooperation

and collaboration. At the international level, it may also serve to facilitate a Whole of System approach" (Klimburg, A. 2012). According to the authors, a national strategy must discuss the link of the strategy not only with strategies, but also with other main documents: internationally and regionally – with conventions, directives, etc., and nationally – with laws and other key documents. This section should differ from a discussion of the national situation, because this section describes how specifically a national cyber security strategy should be integrated into the general system of legal acts/strategic documents.

In the context in question, the following are the main international and regional documents with the provisions of which a national cyber security strategy should be linked: the Convention on Cybercrime ETS No 185; the EU Cyber Security Strategy of 2013; the *Directive* on *Security* of *Network and Information* Systems of 2016 (Article 7 of which provides for concrete requirements for a national security strategy of network and information systems), European Commission Communication of 2016 on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (Strengthening Europe's Cyber Resilience System, 2011) and others.

In addition, a future cyber security strategy of the Republic of Lithuania should comprehensively integrate with the legal acts listed above in this article. All the said documents seek to ensure the highest level of security of the Republic of Lithuania so that common disruptions of operation of particularly important state infrastructures and attacks in the cyber space are best prevented as well as appropriately responded to. Still a part of the documents analysed above speak about security in general terms, while another part is more specifically focused on cyber security. Thus it is believed that a future cyber security strategy of Lithuania should be coordinated with the provisions establishing security in general terms and, in particular, should be coordinated with the conditions which already established cyber security regulation in the Republic of Lithuania. If such a separate section is not provided for in a cyber security strategy, the strategy may "remain" like a separate, detached document the functioning of which will not be integrated into the general system of documents in a state, while non-established links may have a negative impact on the entire system of cyber security planning.

As mentioned above, certain countries have already approved a second cyber security strategy. Lithuania also follows this path – in the next years, a new cyber security strategy should be approved[3]. In this context, it is vital to note that the approval of a new Lithuanian cyber security strategy should take into account the news and differences with the old document – in this particular case – the Lithuanian Cyber Security Programme of 2011 which should be effective until 2019. The critical approach towards the 2011 Programme, already set forth in this article, makes it possible to presume that the new document, a strategy, should have many changes compared with the old document. Therefore, the new strategy must stress concrete essential changes, for instance, introduction of cyber security principles, new strategic priorities and means for ensuring cyber security, etc. Such a comparison would bring much more clarity and would define the trends.

For every national cyber security strategy, including the Lithuanian strategy, a plan of implementation measures is important. The model of the national cyber security strategy selected by the authors is a high-level planning document defining the main objectives and the main measures for an appropriate country in the area of cyber security. Having chosen such a model, it is even more important to also have concrete provisions of implementation. Such provisions may be integrated into a national strategy or presented as a separate document. According to the authors, a plan of measures in Lithuania could be a separate document because a review of the plan of measures should be conducted more often than a review of the strategy itself. To sum up, Figure 4 provides a graphical model of a Lithuanian national cyber security strategy. Based on the various research results, some areas of the model of the national cyber security strategy could be unified and applied in the strategies of other countries (dark blue means that these parts should be mostly unified, and bright blue implies that in such cases national aspects should play the major role).

[3] As mentioned in this article, the question as to the 2011 Lithuanian Cyber Security Programme satisfies the attributes of a strategy will not be considered in detail.

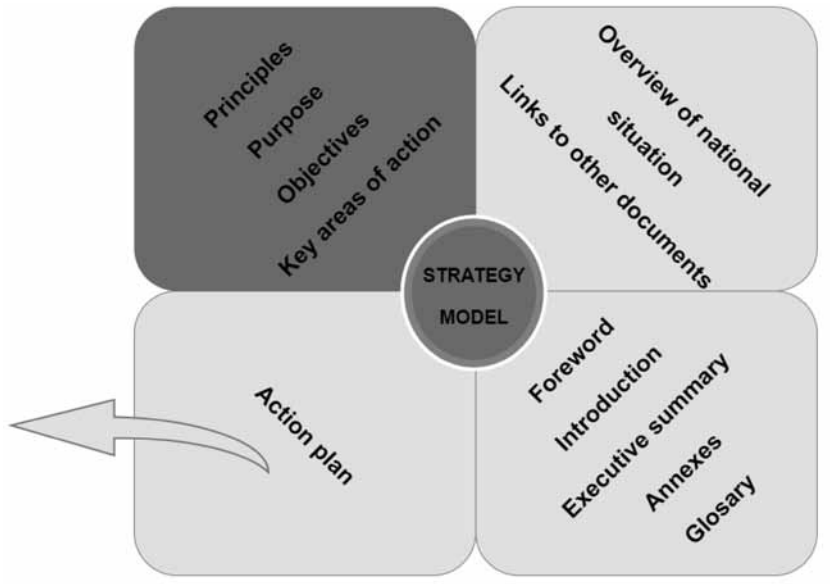

Fig.5. Areas of the Model of a Lithuanian National Cyber Security Strategy.

Source: Designed by the authors.

The validity term of a strategy is also a very important aspect. Based on the results of the conducted survey, the strategy should be effective for up to 5 years; however, it should be reviewed within a shorter period of time. For countries that do not have update mechanisms, the formulation of a NSS or NCSS may become a one-time exercise, dependent on political will to be updated and remain valid. Thus, such strategies run a substantial risk of becoming irrelevant with the passage of time (Klimburg, A. 2012). Therefore, a Lithuanian cyber security strategy should also respond to, for instance, the changes in technology which are applied in ensuring cyber security. In the event where a plan to implement the strategy is approved in addition to the strategy, this plan should be reviewed on an annual basis. The experts pointed out that details become obsolete very fast, for this reason, it is necessary to review them regularly.

When evaluating future cybersecurity strategy of Lithuania, current cybersecurity law and appropriate provisions of the laws ae very important. Assessing the Law on Cyber Security of the Republic of Lithuania which entered into force on 1 January 2015, namely how much the effective law is in conformity with a model developed by the authors[4], first of all it is noteworthy that this law could be amended/supplemented in a few places in the context of the model. The law says that cyber security is based on the general principles of law, the principles of regulation of operation of electronic communications and the following cyber security principles: non-discrimination of cyber space, proportionality of cyber security and supremacy of public interest (Law on Cyber Security of the Republic of Lithuania). While applying legal norms regulating cyber security, all the said principles should be appropriately taken into account. These principles should be coordinated among themselves, and none of them is given priority in advance. Coordination of the principles is undoubtedly necessary. In particular, taking into consideration the fact that based on the principles laid down in the model of the strategy, the law should be supplemented with additional principles, for instance, protection of fundamental rights. According to the authors, the law should provide for, in an adapted manner, all the principles mentioned in the model.

Secondly, even though the law clearly speaks about the institutional cyber security system, it is noteworthy that the National Cyber Security Centre is a structural unit of the Ministry of National Defence of the Republic of Lithuania and is not a *de jure* independent institution. An independent institution should be provided for in Lithuania. The State Data Protection Inspectorate could be an example here, as an institution which is currently accountable to the Government of the Republic of Lithuania.

[4] Which is presented in this article in a brief and shortened manner.

Thirdly, the law should have provisions regarding cyber defence. Currently, cyber defence has been left out of the law altogether. To a certain extent, as much as this is related to the critical infrastructure or state information resources, elements of cyber defence are regulated in secondary legal acts. However, the law needs provisions not only on defence in certain sectors, but also on cyber defence in all the state, including all the possible interested parties.

And fourthly, the law should regulate, in more detail, cooperation at various levels, both within a state among different entities and outside, i.e. with international entities. As mentioned above, cooperation, bearing in mind threats for which borders are non-existent, is one of the main elements in the fight against cyber threats.

Conclusions

Cyber security comparatively a new phenomenon the importance of which is constantly increasing. In this context, timely measures meeting the necessary standards for the fight against cyber incidents should urgently emerge at the national level, and that should take place in a planned manner by efficiently using the available resources and introducing innovation. For this reason, a national cyber security strategy is becoming more important because it is a key planning document defining the main cyber security developments and priority measures in a state.

A national cyber security strategy, as a strategic planning document, should be one of the essential documents in each state providing for the fundamentals and measures of ensuring cyber security as well as priorities of its improvement. The application of a unified cyber security strategy is hindered by national specific features. Regardless of certain sections of a typical national cyber security strategy, which are possibly to be unified, a national cyber security strategy should clearly reflect both the national context and external cyber threats emerging for a particular state.

The national context in the area of cyber security could be linked to various indicators. In Lithuania, this context is manifested through usage of e-services and prevalence of electronic communication networks (especially optical). Besides, in the case of Lithuania, the geopolitical context is clearly seen, i.e. cyber threats emerging from certain neighbouring countries. In addition to the specific features mentioned, each country has a distinctive legal system. The Lithuanian feature is the following – a new Law on Cyber Security took effect as from 1 January 2015, which eliminated the void in fundamental legal regulation in the area of cyber security that existed before. It is thanks to this law that a process of identification of particularly important infrastructure was initiated in Lithuania, which was not yet over during the preparation of this publication. All the specific features mentioned should be reflected in the Lithuanian national cyber security strategy.

The unification of national cyber security strategies has been crucial recently. For instance, if the principles of strategies differ, countries will hardly find efficient mechanisms to fight cyber threats when cooperating among themselves. Therefore, it is necessary to unify the strategies as much as possible so that countries have a similar understanding and similar values and find a dialogue as soon as possible. Thus it is vital to cooperate regarding the global phenomenon and unify the strategies in order to manage global cyber threats. Based on studies conducted by the authors, the following sections of a national cyber security strategy could be more unified: principles, purposes, objectives and key areas of action. While other sections of a national cyber security strategy, which have been mentioned, should better reflect the national situation of a particular country. This is necessary, because cybersecurity drivers and threats vary across countries (National Cybersecurity Strategy Guide, 2012).

Taking into account that usually 85–90 per cent of the cyber infrastructure is managed by the private sector, it is vital to ensure uninterrupted operation of this infrastructure and its resilience to cyber attacks. For this reason, the private sector should be involved both in strategic planning documents and in the real process of cooperation. Strategic alliances between public and private parties would inevitably be the next necessary step to fight cybercrime and maintain cybersecurity (Tropina T., Callanan C. 2015).

Based on the studies conducted, the authors proposed guidelines for a model of the Lithuanian national cyber security strategy and separate sections of the model. These guidelines are based on a number of studies performed, the national specific features of Lithuania and the analysis of the legal environment of Lithuania. The guidelines provide proposals regarding the main sections of the Lithuanian cyber security strategy and specific features of the content of these sections. These proposals are also particularly relevant because Lithuania's strategic document is probably one of the weakest currently. The Lithuanian Cyber Security Programme, which should be in effect until 2019, is in least conformity with the provisions of strategic documents in the area of cyber security of the EU and NATO among all the countries of the EU and NATO. Taking into account the national context and the geopolitical situation, which is becoming more heated, Lithuania should hurry up and adopt a new contemporary cyber security strategy. Besides, the Law on Cyber Security of the Republic of Lithuania should be appropriately amended and supplemented because even though it took effect at the beginning of 2015, unfortunately, it is not in full conformity with a model of the strategy proposed by the authors: the key discrepancies are related to principles, the institutional structure, cyber defence and cooperation.

Similar countries, when drawing up or updating their national cyber security strategies, should cooperate more and exchange the best practice; they should also take over the best practice of other countries, however, following its adaptation considering the national situation. Such a model should improve the global fight against cyber incidents and better ensure both regional and national cyber security interests.

Acknowledgements

The authors are grateful for the Research Council of Lithuania which funded this article as a part of the study "Analysis and Adaptation of EU and NATO Cyber Security Strategies: The Lithuanian Cyber Security Strategy Model" (a grant No MIP-099/2015).

References

Approval of the Programme for the Development of Electronic Information Security (Cyber Security) for 2011–2019". Official Gazette Valstybės Žinios, No 83-4033, 2011; No 106 (correction).

Assessment of threats to national security. State Security Department of the Republic of Lithuania and 2nd department of operational services under the Ministry of National Defence. Vilnius. Available on the Internet: <http://www.vsd.lt/Files/Documents/635948635773762500.pdf>

Belás, J.; Korauš, M.; Kombo, F.; Korauš, A. 2016. Electronic banking security and customer satisfaction and in commercial banks, *Journal of Security and Sustainability Issues* 5(3): 411-422. http://dx.doi.org/10.9770/jssi.2016.5.3(9)

Catherine Dale, National Security Strategy. *Legislative Mandates, Execution to Date, and Considerations for Congress* (Washington, DC: Congressional Research Service, 2008). Available on the Internet: <http://fpc.state.gov/documents/organization/106170.pdf>

Cyber security strategies of countries all over the world and years of their adoption may be seen on the ENISA website. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world>

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry" COM(2016)410 final, Brussels, July 5, 2016. Available on the Internet: <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16546>

ENISA NCSS Good Practice Guide, 2016. Available on the Internet: <https://www.enisa.europa.eu/publications/ncss-good-practice-guide>

European Union data. Available on the Internet: <http://www.internetworldstats.com/europa.htm>

Fisher E.A. 2009. *Creating a National Framework for Cybersecurity. An Analysis of issues and Options.* Nova Science Publishers, Inc., New York.

Gasparėnienė, L.; Remeikienė, R.; Sadeckas, A.; Ginevičius, R. 2016. Level and sectors of digital shadow economy: the case of Lithuania, *Entrepreneurship and Sustainability Issues* 4(2): 183-197. http://dx.doi.org/10.9770/jesi.2016.4.2(6)

Government of the Republic of Lithuania, Resolution No 796 of 29 June 2011.

Klimburg, A. 2012. *NATO Cybersecurity Framework Manual*. NATO CCD COE Publication, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.

Korauš, A.; Dobrovič, J.; Ključnikov, A.; Gombár, M. 2016. Consumer approach to bank payment card security and fraud, *Journal of Security and Sustainability Issues* 6(1): 85-102. http://dx.doi.org/10.9770/jssi.2016.6.1(6)

Law on Cyber Security of the Republic of Lithuania. Available on the Internet: <https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4>

National Cybersecurity Strategy Guide. ITU, Geneva, 2012. Available on the Internet: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf>

NATO Chief: Cyber Can Trigger Article 5. Available on the Internet: <http://www.defensenews.com/story/defense/policy-budget/warfare/2015/03/25/nato-cyber-russia-exercises/70427930>

Olaniyi, E. O.; Reidolf, M. 2015. Organisational innovation strategies in the context of smart specialization, *Journal of Security and Sustainability Issues* 5(2): 213-227. http://dx.doi.org/10.9770/jssi.2015.5.2(7)

Operational report of CERT-LT for Quarter II of 2016. Available on the Internet: <https://www.cert.lt/doc/2016_2.pdf, accessed on 26 September 2016>

Schjolberg S., Ghernaouti-Hele S. 2011. *A Global Treaty on Cybersecurity and Cybercrime.* Geneva. Available on the Internet: <http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf>

Štitilis, D.; Pakutinskas, P.; Kinis, U.; Malinauskaitė, I. 2016. Concepts and principles of cyber security strategies, *Journal of Security and Sustainability Issues* 6(2): 197-210. http://dx.doi.org/10.9770/jssi.2016.6.2(1)

Štitilis, D.; Pakutinskas, P.; Malinauskaitė, I. 2016. Preconditions of sustainable ecosystem: cyber security policy and strategies, *Entrepreneurship and Sustainability Issues* 4(2): 174-182. http://dx.doi.org/10.9770/jesi.2016.4.2(5)

Teivāns-Treinovskis, J.; Amosova, J.; Načisčionis, J.; Ņesterova, M. 2016. Country's development and safety: violent crimes in crime structure, *Journal of Security and Sustainability Issues* 6(2): 227-233. http://dx.doi.org/10.9770/jssi.2016.6.2(3)

The official statistics portal. Available on the Internet: <http://osp.stat.gov.lt/web/guest/statistiniu-rodikliu-analize?portletFormName=visualization&hash=d4a59fe4-1794-45fb-9cd5-74e8851081be>

Tropina T., Callanan C. 2015. *Self- and Co-regulation in Cybercrime.* Cybersecurity and National Security. Springer, p. 25.

Vaško, M.; Abrhám, J. 2015. Issues of secure and sustainable e-tourism: case of the Czech Republic, *Journal of Security and Sustainability Issues* 5(2): 137-148. http://dx.doi.org/10.9770/jssi.2015.5.2(1)

World Bank national accounts data, and OECD National Accounts data files. Available on the Internet: <http://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=LT>

Zahars, V.; Stivrenieks, M. 2016. Security and safety enforcment: execution peculiarities, *Journal of Security and Sustainability Issues* 6(1): 71-83. http://dx.doi.org/10.9770/jssi.2016.6.1(5)

Short biographical notes

Darius Stitilis is professor at the Mykolas Romeris University (e-mail: stitilis@mruni.eu). He obtained PhD degree in law from Mykolas Romeris university in 2002 (the topic of Phd Thesis was related to the legal responsibility in cyberspace). He is the executive manager of master study program "Cyber cesurity management" at Mykolas Romeris University. His research interests include IT law, cyber security law, privacy and personal data protection law, electronic identification law, cybercrime. He has over 40 publications primarily in the field of law and IT. Under his direction, he was involved in several scientific EU and national projects. Also, he is the co-author of two scientific monographs regarding identity theft in cyberspace: legal and electronic business issues, and e-health.

OR:
Darius Štitilis
ORCID ID: orcid.org/0000-0002-9598-0712.

Paulius Pakutinskas is associated professor at the Mykolas Romeris University (e-mail: paulius.pakutinskas@mruni.eu). He obtained PhD degree in law from Mykolas Romeris university in 2009 (the topic of Phd Thesis was related to the legal regulation of electronic communications). His research interests include IT law, intellectual property, cyber security. Also, he is the co-author of scientific monographs regarding identity theft in cyberspace: legal and electronic business issues.

OR: **Paulius Pakutinskas**
ORCID ID: orcid.org/0000-0003-2179-5298

Marius Laurinaitis is a lecturer at Mykolas Romeris University (e-mail: laurinaitis@mruni.eu). He obtained PhD degree in law from Mykolas Romeris University in 2015 (the topic of PhD Thesis was related to the Legal Regulation of Electronic Money). He is the executive editor of International Scientific Research Journal "Intellectual Economics". His research interests include IT law, privacy and personal data protection law, electronic identification law, electronic payments law, electronic money. Under his direction, he was involved in scientific EU and national projects.

OR: **Marius Laurinaitis**
ORCID ID: orcid.org/0000-0002-2926-9260

Inga Malinauskaitė is a lecturer and PhD student at the Mykolas Romeris University (e-mail: inga.malinauskaite@mruni.eu). Her PhD topic is related to regulation and protection of data subject's rights in online social networks. Her research interests include data subject's rights, data protection in relation to IT systems, intellectual property, cyber security, online security issues.

OR: **Inga Malinauskaitė**
ORCID ID: orcid.org/0000-0001-5693-7300