INDEPENDENT JOURNAL OF MANAGEMENT & PRODUCTION (IJM&P)
http://www.ijmp.jor.br v. 11, n. 9, Special Edition (Baltic States), November 2020
ISSN: 2236-269X
DOI: 10.14807/ijmp.v11i9.1431

NATIONAL CYBER SECURITY STRATEGIES: MANAGEMENT, UNIFICATION AND ASSESSMENT

Darius Štitilis
Mykolas Romeris University, Lithuania
E-mail: stitilis@mruni.eu

Irmantas Rotomskis
Mykolas Romeris University, Lithuania
E-mail: marius@laurinaitis.eu

Marius Laurinaitis
Mykolas Romeris University, Lithuania
E-mail: marius@laurinaitis.eu

Sergiy Nadvynychnyy
Ternopil National Economic University, Ukraine
E-mail: nsa2008@ukr.net

Nadiya Khorunzhak
Ternopil National Economic University, Ukraine
E-mail: n.khorunzhak@ukr.net

Submission: 8/21/2020
Revision: 9/04/2020
Accept: 9/05/2020

ABSTRACT

Cyber security has become an important issue both on the EU and the national level. Cyber security is now perceived as a part of national security. The newly emerging cyber security policy, comprising national cyber security strategies as an important constituent part, has been recently paid considerable attention. Speaking of national cyber security strategies, a positive thing is that the majority of EU member states have already approved such strategies. However, the approved strategies differ considerably in terms of their content and implementation. The present article aims at identifying reasons for differences in individual national strategies and analyses aspects of their unifications in expectation to find out an optimum balance between the degree of unification and the need to retain differences arising from intrinsic national singularities. To this end, the article analyses the issue of national cyber security on the basis of Lithuania's cyber security strategy as a sample in the context of ENISA good practices for the development of cyber security strategies and by application of ENISA developed KPIs and testing ENISA cyber security strategy evaluation tool. Finally, the article suggests recommendations on further development of national cyber security strategies in terms of their unification and national singularities.

Keywords: Cyber security; National cyber security strategy; Cyber security policy; Management

1. INTRODUCTION

Cyber threats have become an issue of major concern both on the national and international level. Scientific research emphasizes the global nature of the cyber space predetermining the global character of the possible threats. Because of the global character, investigation in cyber incidents or attacks becomes complex and sometimes impossible. It has to be noted though that cyber-attacks actually take place in a particular territory and involve physical subjects located in a specific territory as well and are committed by natural or legal persons subject to particular national jurisdictions (SCHMITT, 2017). One may suggest to deal with the problem by coordinating cyber security policies on the global/regional level; however, the importance of national regulation in combating cyber threats may not be neglected as well.

Development of the cyber security policy has been paid considerable attention by the EU. In 2016, the EU adopted 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, which became a major instrument helping unify cyber security policies of nation states. On 13 September 2017 the Commission adopted a cybersecurity package.

The Cybersecurity Act, which has now entered into force, lay at the core of the package. The changes this new EU regulation brings about are twofold: a comprehensive reform of ENISA and the creation of a certification framework (CYBER SECURITY. EUROPEAN COMMISSION).

An important role in the development of the cyber security policy is played by national cyber security strategies. The national strategies are actually one of the measures to ensure cyber security. Technologies and techniques, strategies and tactics, motives and ideologies, rules and laws, institutions and industries, power and money - all of these topics have a role to play in cybersecurity, and all of these are tightly interwoven (TROPINA; CALLANAN, 2015).

National cyber security strategies are becoming more and more important. Individual nation states invest significant efforts into development of their cyber security strategies. At the moment, approved national cyber security strategies may be found in all EU member states. The situation may be well illustrated by ENISA cyber security strategy interactive map, publicly available at (NATIONAL CYBER SECURITY STRATEGIES – INTERACTIVE MAP. ENISA). The map includes objectives set in individual national strategies. Already having looked at the objectives, one may spot differences in the numbers and the content. In the following chapters, the article describes an approach to national cyber security strategies as well as their unification and national singularities.

2. LITERATURE REVIEW

2.1. Endeavors to coordinate cyber security policies in combat against cyber attacks

Endeavours to combat cyber threats now being made on the EU level. In 2013, the EU adopted European cyber security strategy (AN OPEN, SAFE AND SECURE CYBERSPACE, 2013). The strategy aims at making the EU digital environment the safest in the world and protecting major values and freedoms. It sets five major objectives: I) to improve cyber immunity, ii) to reduce the cybercrime rate, iii) to establish and further develop a cyber-defence policy, iv) to build up industrial and technological resources and v) to establish an international cyber space policy compliant with core values of the EU.

The European cyber security strategy was further extended by adopting several subsequent instruments:

- *The European Agenda on Security* (THE EUROPEAN AGENDA ON SECURITY, 2015) with the purpose to help judicial authorities and law enforcement agencies to respond to cybercrime, mainly by renewing policies and amending legal acts. The agenda also set goals to identify obstacles for criminal investigations and improve development of cyber capabilities.
- *A Digital Single Market Strategy for Europe* (A CONTEST FOR EASTERN EUROPE, 2015) with the purpose to create better opportunities to use digital products and services by means of creating proper conditions to exploit the potential of the digital economy growth. To this end, improvement of security, reliability and inclusion of the Internet is essential.
- *A Global Strategy for the European Union's Foreign and Security Policy 2016* with the purpose to strengthen the EU's role as a global actor. Cyber security has become a major pillar in today’s commitment to cyber development, cooperation with key partners and

determination to deal with cyber issues in all spheres of politics, including tackling disinformation by means of strategic communication.

Issues of national cyber security strategies are out of the scope of the aforementioned instruments. However, it is important to note that the approach to cyber security and policy development should be wider to comprise national security aspects and other dimensions including disinformation and general threats.

One of the key binding instruments is Network and Information Security directive of 2016, which laid down fundamentals for cyber security systems in all EU member states, ranging from standards of national cyber security strategies to the requirements for national CERTs. In fact, the directive harmonizes the content of national cyber security strategies.

First, the directive lays down a general obligation for member states to introduce national cyber security strategies. Second, the directive stipulates more explicit requirements in Article 7: The national strategy on the security of network and information systems primarily addresses the following issues:

a) the objectives and priorities of the national strategy on the security of network and information systems;
b) a governance framework to achieve the objectives and priorities of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors;
c) the identification of measures relating to preparedness, response and recovery, including cooperation between the public and private sectors;
d) an indication of the education, awareness-raising and training programmes relating to the national strategy on the security of network and information systems;
e) an indication of the research and development plans relating to the national strategy on the security of network and information systems;
f) a risk assessment plan to identify risks;
g) a list of the various actors involved in the implementation of the national strategy on the security of network and information systems.

Member States may turn to ENISA for advice and assistance when developing their national strategies. As per article 7(3) Member States ought to communicate their national strategies to the Commission within three months from their adoption (MARKOPOULOU; KONSTANTINOU; DE HEART, 2019).

However, the directive is not likely to explicitly regulate obligations of nations states in terms of national cyber security strategies. In fact, the aforementioned obligations leave nation states considerable freedom in the development of their national cyber security strategies. Yet, according to the directive, at least key requirements laid down in Article 7 must be followed.

The directive had to be transposed into national law of EU members states by 2018. Most of the member states have already transposed the directive into their legislation (NIS IMPLEMENTATION TRACKER, 2020), mostly in 2018. Although effective only for two years, the directive is already likely to yield positive results. It has to be noted though that the correlation between cyber incidents and the legal environment is difficult to evaluate, and it is not the object of this study to research the causal links. However, speaking of the latter, the statistics shows no decline in cyber risks (CYBERSECURITY STATISTICS FOR 2020).

2.2. National cyber security strategies and their differences

So far, the creation and development of national cyber security strategies have been little coordinated. The strategies considerably differ in a range of aspects, including the key principles, goals, objectives and specific implementation measures. Some of them contain principles, goals and measures that are completely absent in strategies developed by other nation states. Descriptions of the strategies also differ: some of them are very explicit while others are much shorter, specifying in detail only, for example, the principles and objective.

Differences may also be observed in other aspects, such as the way of enforcement, legal status, termination, etc. Differences in national cyber security strategies have been evidenced by scientific study as well (ŠTITILIS; PAKUTINSKAS; MALINAUSKAITĖ, 2016). Reasons of the observed differences vary. It may be the level of the state's maturity in the field (SABILLON et al., 2016) or it may be predetermined by different understanding of cyber security, specific national situations, etc.

At the moment, the process of adoption of the second or even the third strategy may be observed among various nation states. However, the newly adopted strategies still tend to retain considerable differences. Thus, as differences between provisions of individual national strategies remain, a uniform cyber security policy is still unlikely to emerge. Having in mind the fact that cyber threats are often of an international nature, the differences are likely to hinder development of a common regional or international cyber security policy.

Harmonization of national cyber security strategies may be insufficient as even on implementation of the directive provisions, individual strategies are likely to retain significant differences.

However, certain differences among national cyber security strategies may not be avoided as individual nation states may face specific cyber threats. Along with conventional cyber threats, today's security issues already include hybrid threats. For example, the Baltic states are constantly facing adverse propaganda disseminated by Russia. Propaganda may often be part of the so-called cyber war.

According to a recent study on hybrid threats, the Russkiy Mir Foundation (RMF) is a cultural and educational institution that promotes Russian language and culture across over 100 countries. RMF has constructed a network of influencers among NATO nations, especially those bordering the Russian Federation. Such organisations are capable of activity which is hostile to the host nation and may contribute to cleavages in those societies (HYBRID THREATS: A STRATEGIC COMMUNICATIONS PRESPECTIVE, 2019). Thus, having in mind the wider context comprising national security aspects, such threats should also be described in national cyber security strategies along with relevant measures ensuring security of the cyber space.

Another example of specific threats may be observed in countries generating nuclear power, which have to deal with specific safety issues. Cyber threats are among possible threats in nuclear industry (NUCLEAR ENERGY AND CURRENT SECURITY ENVIRONMENT IN TH AREA OF HYBRID THREATS, 2019), to be considered on the national level. Certain electronically controlled nuclear power systems include safety control systems, which may be targeted by cyber attackers. Thus, issues of nuclear safety must be taken into consideration by planners of cyber security measures even on the national scale.

Differences may also be associated with the development and the state of the electronic communications infrastructure, singularities of legal regulation, etc.

2.3. ENISA's role in harmonization of national cyber security strategies

ENISA’s work in supporting these strategies has focused on the analysis of existing NCSS; on the development and implementation of NCSS; on outlining and raising awareness of good practice to provide guidance and practical tools to the Member States for evaluating their NCSS (VENUTI TRANSLATION STRATEGY) To this end, ENISA provided recommendations or guidelines for good practices of the development of national cyber security strategies. In summary, it should be noted that most productive ENISA activities, in terms of the provided recommendations/guidelines, took place in the period from 2012 to 2016. The list of ENISA activities is presented below.

Table 1: ENISA recommendations/guidelines for national cyber security strategies

Name	**Year**	**Description**
National Cyber Security Strategy Good Practice Guide	2012, 2016	This guide is updating the different steps, objectives and good practices of the original guide and analyses the status of NCSS in the European Union and EFTA area. The aim is to support EU Member States in their efforts to develop and update their NCSS. Therefore, the target audience of this guide are public officials and policy makers. The guide also provides useful insights for the stakeholders involved in the lifecycle of the strategy, such as private, civil and industry stakeholders (NCSS GOOD PRACTICE GUIDE).
National Cyber Security strategies	2012	The paper includes a short analysis of the current status of cyber security strategies within the European Union and elsewhere. It also identifies common themes and differences, and concludes with a series of observations and recommendations. The paper is based on the preliminary findings and analysis from an ENISA project that is working to develop a Good Practice Guide on how to develop, implement and maintain a national cyber security strategy (NATIONAL CYBER SECURITY STRATEGIES).
National Cyber Security Strategies: An Implementation Guide	2012	This report introduces a set of concrete actions, which if implemented will lead to a coherent and holistic national cyber-security strategy. It also proposes a national cyber-security strategy lifecycle, with a special emphasis on the development and execution phase. For each component of the strategy a list of possible and indicative Key performance indicators (KPIs) will be described. Senior policy makers will find practical recommendations on how to control the overall development and improvement process and how to follow up on the status of national cyber-security affairs within their country(NATIONAL CYBER SECURITY STRATEGIES).
Updated NCSS Good Practice Guide	2016	This guide is updating the different steps, objectives and good practices of the original guide and analyses the status of NCSS in the European Union and EFTA area. The aim is to support EU Member States in their efforts to develop and update their NCSS. Therefore, the target audience of this guide are public officials and policy makers. The guide also provides useful insights for the stakeholders involved in the lifecycle of the strategy, such as private, civil and industry stakeholders (NCSS GOOD PRACTICE GUIDE).

Source: compiled by the authors

It can be stated that the aforementioned ENISA documents considerably contributed to formation of good practices in national cyber security strategies. However, as differences in national cyber security strategies show, unification of the strategies is still insufficient. It is very important for nation states to evaluate how specific strategies comply with ENISA formed good practices. Such evaluation may be done by means of a newly ENISA developed evaluation tool.

By 2018, ENISA created National Cyber Security Strategies evaluation tool to help Member States evaluate their strategic priorities and objectives related to National Cyber Security Strategies. The tool incorporated fifteen objectives, developed and presented in the aforementioned guidelines of 2016:

- Develop national cyber contingency plans
- Protect critical information infrastructure

- Organise cyber security exercises
- Establish baseline security measures
- Establish incident reporting mechanisms
- Raise user awareness
- Strengthen training and educational programmes
- Establish an incident response capability
- Address cyber crime
- Engage in international cooperation
- Establish a public-private partnership
- Balance security with privacy
- Institutionalise cooperation between public agencies
- Foster R&D
- Provide incentives for the private sector to invest in security measures.

The objective of this investigation - to assess EU cyber security policy and the potential for unifying national cyber security strategies.

3. DATA AND METHODOLOGY

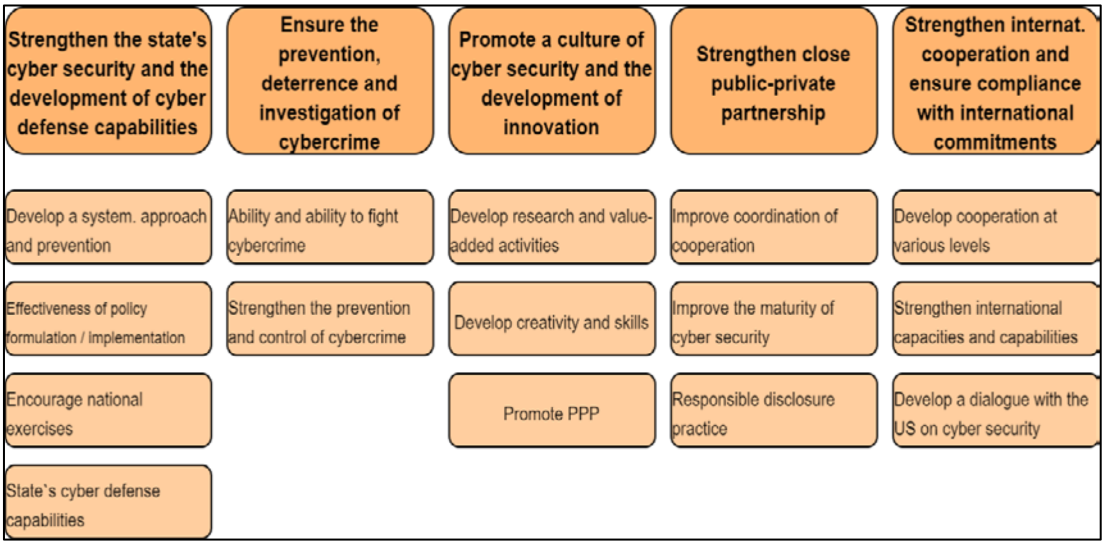
In preparing this article and presenting the outcomes of research, the authors used several methods, including analysis of legal regulation related to cyber security strategies and appropriate generalizations. The results of the comparative study of cyber security strategies were used, and the ENISA tool for evaluating cyber security strategies was analyzed.

The authors also used a modelling method. Based on the ENISA cyber security strategy evaluation tool, the situation was modelled in comparison with the Lithuanian cyber security strategy model.

4. RESULTS

4.1. National Cyber Security Strategies evaluation tool: example evaluation of Lithuanian national cyber security strategy

To illustrate how the evaluation tool actually works, we chose an example of Lithuania's national cyber security strategy of 2018, approved by Decision No 818 of the government of the Republic of Lithuania in 2018. Compared to equivalent cyber security strategies of other nation states (which often are just a set of cyber security principles), the strategy is actually an explicit and detailed document. The document is structured to include key objectives and goals which may be described as follows:



Strengthen the state's cyber security and the development of cyber defense capabilities	Ensure the prevention, deterrence and investigation of cybercrime	Promote a culture of cyber security and the development of innovation	Strengthen close public-private partnership	Strengthen internat. cooperation and ensure compliance with international commitments
Develop a system. approach and prevention	Ability and ability to fight cybercrime	Develop research and value-added activities	Improve coordination of cooperation	Develop cooperation at various levels
Effectiveness of policy formulation / implementation	Strengthen the prevention and control of cybercrime	Develop creativity and skills	Improve the maturity of cyber security	Strengthen international capacities and capabilities
Encourage national exercises		Promote PPP	Responsible disclosure practice	Develop a dialogue with the US on cyber security
State`s cyber defense capabilities				

Figure 1: Objectives and goals of the national cyber security strategy of Lithuania
Source: compiled by the authors

As the objectives and goals are planned explicitly and in detail, the strategy may seem at the first sight to reflect of include all ENISA good practice objectives and implementation recommendations. Analysis of Lithuania's cyber security strategy may be good example to be followed by other countries.

The explicit evaluation of Lithuania's national cyber security strategy by means of the ENISA tool is given below. The ENISA evaluation tool was used to mark all the 15 objectives to be checked against criteria set in the ENISA model.

The results revealed that according to ENISA developed tool, Lithuania's national cyber security strategy still retains many places to be improved. The table below describes KPI`s (i.e. objectives) specifying if the ENISA tool contains recommendations on each of the objectives[1].

[1] However, it has to be noted that in case of a positive answer, the level of ENISA KPI implementation may differ. Thus, recommendations and the number of recommendations may as well be different. However, the table contains only general answers, which only reveal if a specific objective set by means of the ENISA tool was given recommendations testifying that a certain deficiency was identified.

ISSN: 2236-269X
DOI: 10.14807/ijmp.v11i9.1431

Table 2: Recommendations on specific objectives (present/absent)

Objective	**Are recommendations given? Yes/No**
Develop national cyber contingency plans	Yes
Protect critical information infrastructure	Yes
Organise cyber security exercises	Yes
Establish baseline security measures	Yes
Establish incident reporting mechanisms	Yes
Raise user awareness	Yes
Strengthen training and educational programmes	Yes
Establish an incident response capability	No
Address cyber crime	Yes
Engage in international cooperation	Yes
Establish a public-private partnership	Yes
Balance security with privacy	No
Institutionalise cooperation between public agencies	Yes
Foster R&D	Yes
Provide incentives for the private sector to invest in security measures	No

Source: compiled by the authors

Thus, only three areas of Lithuania's national cyber security strategy may be deemed fully compliant with ENISA good practice. Al the remaining areas were subject to certain recommendations on incompletely implemented ENISA suggested good practices.

The experiment with Lithuania's national cyber security strategy has revealed that despite being explicit and detailed, the strategy may still contain areas to be improved, 12 of 15 objectives in this particular case. Although all the objectives may be found in Lithuania's national cyber security strategy, their specific description still needs to be improved and supplemented by additional measures.

However, it has to be noted that the ENISA evaluation tool sets identical KPIs and evaluation principles for all nation states. The method actually fails to evaluate if an individual nation state identifies certain singularities in their cyber security situation and if such singularities are considered in their cyber security strategies. One may doubt if such technique is the right way to evaluate individual cyber security strategies.

After all, nations states can be different in a variety of aspects, ranging from the size, population and financial capacities to introduce necessary safety measures to specific cyber threats predetermined by exterior factors, geographical location and cybercrime rate. How different the situation in the field of e-crime may be can be observed in Eurobarometer data published in 2019 (EUROPEANS’ ATTITUDES TOWARDS INTERNET SECURITY, 2019).

4.2. The model of Lithuania's national cyber security strategy

Prior to adoption of Lithuania's national cyber security strategy, a model of Lithuania's national cyber security strategy was developed (THE MODEL OF LITHUANIA'S NATIONAL CYBER SECURITY STRATEGY, 2017).

Among other questions, the model, designed specifically for an individual country (Lithuania in this particular case), emphasizes the necessity to take into account the national situation in Lithuania. In other words, a national cyber security strategy must be developed in view of the specific national situation. In Lithuania's case, the following key elements may be distinguished:

- cyber threats in Lithuania in terms of the geopolitical situation;
- electronic public services and e-business in Lithuania;
- legal environment, including national programs and strategies in the field of IT security and electronic data protection.

One of the specific things that can be mentioned in Lithuania's case is the that some of its critical infrastructure units are using SCADA information systems. The systems contain certain elements prone to security risks, e.g. an opportunity to interfere with the security systems.

A good example may be the Stuxnet case where a computer worm has been used against Iran's nuclear program. Thus, the use of such systems, particularly in a critical infrastructure, incurs specific cyber security risks, which have to be taken into consideration when developing a national cyber security strategy. It is attributable to national singularities as SCADA systems are mostly used in Eastern European countries.

It has to be noted though, that the aforementioned elements identified in Lithuania's case may coincide with, be similar to or essentially differ from elements describing national singularities of other countries and may depend on political, economic and cultural factors.

In our opinion, it is essential for the developers of national cyber security strategies to take into consideration national singularities of individual nation states. The national singularities should also be included into ENISA KPIs and the ENISA evaluation tool. This would help nation states to develop adequate cyber security strategies suitable for their individual situations.

Further research might focus on the development of methodologies suitable for identification of singularities of individual nation states in the context of cyber security so as to allow evaluation of the needs and development of cyber security systems actually responding to the real situation and real cyber threats.

5. CONCLUSIONS

While issues of cyber security are quite explicitly coordinated on the EU level, regulation of national cyber security strategies is still minimal. National cyber security systems should undergo unification in view of the fact that cyber security threats often go beyond the boundaries of national borders and are, generally speaking, global, presenting essentially similar challenges to all nation states.

Legal regulation should be further developed on the EU level or on the level of recommendations so as to uniform national cyber security strategies, which have a significant impact both on the situation in the national cyber security and on safeguarding cyber security on the regional or international level.

However, unification of national cyber security strategies is still subject to certain restraints, that is they have to reflect inevitable national singularities. To put it other way, the strategies should also focus on national singularities identified by nation states alone. Although cyber threats are essentially of an international nature, national singularities, such as the geopolitical location, the developed electronic communications infrastructure, the national legal environment, etc., may have a significant role in ensuring cyber security and thus have to be reflected in the national cyber security strategy.

Good practices provided by ENISA for the development of national cyber security strategies have to put a greater emphasis on differences between individual strategies, predetermined by national singularities. Moreover, ENISA National Cyber Security Strategies evaluation tool should also comprise national singularities which may be important for cyber security situation in a particular country. Thus, the methodology of ENISA evaluation tool should also be improved.

Modern high quality national cyber security strategies capable of dealing with today's cyber threats are only viable by additionally highlighting national singularities attributable to a cyber-security situation in a particular nation state.

REFERENCES

A DIGITAL SINGLE MARKET STRATEGY FOR EUROPE. COM (2015) **192 final**. Brussels, 2015. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015DC0192&from=LT. Access: 20 May 2020

A GLOBAL STRATEGY FOR THE EUROPEAN UNION'S FOREIGN AND SECURITY POLICY (2016) http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_lt_.pdf

CYBER SECURITY. EUROPEAN COMMISSION (2020) https://ec.europa.eu/digital-single-market/en/policies/cybersecurity. Acess: 15 April 2020

CYBER SECURITY STRATEGY OF THE EUROPEAN UNION (2013) **An Open, Safe and Secure Cyberspace**. JOIN (2013) final 1. Available: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf. Access: 25 June 2020

HYBRID THREATS: A STRATEGIC COMMUNICATIONS PRESPECTIVE (2019) NATO Strategic Communications Centre of Excellence (**NATO StratCom COE**), 124 p. https://stratcomcoe.org/hybrid-threats-strategic-communications-perspective

LITHUANIA'S NATIONAL CYBER SECURITY STRATEGY OF 2018 (2018) approved by Decision No 818 of the government of the Republic of Lithuania in 2018. Available: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/94365031a53411e8aa33fe8f0fea665f?jfwid=dg8d31595. Access: 20 May 2020

MARKOPOULOU, D.; KONSTANTINOU, P.; DE HEART, P. (2019) **The new EU cybersecurity framework**: The NIS Directive, ENISA's role and the General Data Protection Regulation // Computer Law & Security Review, November 2019, Volume 35, issue 6. Available: https://www.sciencedirect.com/science/article/pii/S0267364919300512?via%3Dihub. Access: 20 May 2020

MUST-KNOWN CYBERSECURITY STATISTICS FOR 2020 (2020) Available: https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/. Access: 22 May 2020

NATIONAL CYBER SECURITY STRATEGIES – INTERACTIVE MAP. ENISA Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map. Access: 24 May 2020

NATIONAL CYBER SECURITY STRATEGIES: AN IMPLEMENTATION GUIDE (2020) Available: https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide. Access: 05 June 2020

NATIONAL CYBERSECURITY STRATEGIES. ENISA (2020) Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies. Access: 20 May 2020

NATIONAL CYBER SECURITY STRATEGIES. ENISA (2020) Available: https://www.enisa.europa.eu/publications/cyber-security-strategies-paper. Access: 28 May 2020

NCSS GOOD PRACTICE GUIDE. ENISA (2020) Available: https://www.enisa.europa.eu/publications/ncss-good-practice-guide. Access: 27 May 2020

NIS IMPLEMENTATION TRACKER (2019) Available: https://www.digitaleurope.org/resources/nis-implementation-tracker/. Access: 27 May 2020

NUCLEAR ENERGY AND CURRENT SECURITY ENVIRONMENT IN TH AREA OF HYBRID THREATS (2019) **Research report**. The European Centre of Excellencefor Countering Hybrid Threats. Available: https://www.stratcomcoe.org/nuclear-energy-and-current-security-environment-era-hybrid-threats. Access: 10 June 2020

SABILLON, R.; CAVALLER, V.; CANO, J. (2016) National Cyber Security Strategies: Global Trends in Cyberspace **International Journal of Computer Science and Software Engineering (IJCSSE),** v. 5, n. 5, p. 67-81. Available: <http://ijcsse.org/published/volume5/issue5/p1-V5I5.pdf>. Acess: 14 April 2020

SCHMITT M. N. (2017) **Tallin Manual 2.0 on the International Law Applicable to Cyber Operations**. Cambridge University Press. Available: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf. Access: 24 May 2020

SPECIAL EUROBAROMETER 480. EUROPEANS' ATTITUDES TOWARDS INTERNET SECURITY (2019) Available: <http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/85495>. Access: 10 April 2020

ŠTITILIS, D.; PAKUTINSKAS, P.; LAURINAITIS, M.; MALINAUSKAITĖ, I. (2017) A model for the national cyber security strategy. The Lithuanian case, **Journal of Security and Sustainability**, v. 6, n. 3, p. 357-372. https://doi.org/10.9770/jssi.2017.6.3(3).

ŠTITILIS, D.; PAKUTINSKAS, P.; MALINAUSKAITĖ, I. (2016) **EU and NATO cybersecurity strategies and national cybersecurity strategies**: a comparative analysis**. Security Journal**, v. 30, n. 4. DOI: 10.1057/s41284-016-0083-9.

THE EUROPEAN AGENDA ON SECURITY. COM (2015) **185 final**. Strasbourg. Available: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf. Access: 29 June 2020

TROPINA, T.; CALLANAN, C. (2015) **Self- and Co-regulation in Cybercrime, Cybersecurity and National Security.** Springer.