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
2015 September Volume 5 Number 1
http://dx.doi.org/10.9770/jssi.2015.5.1(4)

ASPETS OF CYBERSECURITY: THE CASE OF LEGAL REGULATION IN LITHUANIA

Darius Štitilis, Valdas Klišauskas

Mykolas Romeris University, Ateities str. 20, LT-08303 Vilnius Lithuania

Emails: stitilis@mruni.eu, valdas.klisauskas@gmail.com

Received 20 March 2015; accepted 26 July 2015

Abstract. Lately a lot of attention has been given to legal regulation of cybersecurity. This article will review legal regulation of cybersecurity in Lithuania. Historical retrospective of legal regulation of cybersecurity in Lithuania will be discussed, strategic Lithuanian cybersecurity documents will be analysed, and the Law on Cybersecurity of the Republic of Lithuania will be analysed and evaluated. After a comparative analysis of cybersecurity strategies and laws and a review of legal regulation of cybersecurity in Lithuania, gaps of law-making and of other measures were distinguished, and corresponding conclusions were made. The adoption of the new Law on Cybersecurity, which regulates many important institutes, is evaluated positively. But with regard to the current legal regulation on cybersecurity in Lithuania additional measures are necessary (functions of institutions that formulate cybersecurity policy and perform control functions have not been detailed and distinguished, also functions of the Lithuanian national Computer Emergency Response Team (CERT) are not foreseen in the Law on Cybersecurity, etc.).

Keywords: cybersecurity, legal regulation, strategies, law.

Reference to this paper should be made as follows: Štitilis, D.; Klišauskas, V. 2015. *Journal of Security and Sustainability Issues* 5(1): 45–57. DOI: http://dx.doi.org/10.9770/jssi.2015.5.1(4)

JEL Classifications: K29

1. Introduction

Factors that determine a country's security and their relation with sustainable development processes are widely analysed in contemporary scientific literature (e.g. Stańczyk 2011; Lankauskienė, Tvaronavičienė 2012; Wahl, M.; Prause, 2013; Vosylius *et al.* 2013; Wahl 2014; Grubicka, Matuska 2015). Cybersecurity is one of the components of a country‘s security.

Development of information technologies and transfer of information into cyberspace increases the quality of information processes and activities as well as ensures better competitiveness and efficiency. But this also leads to negative consequences, such as loss of important electronic information or even cybercrime. As the number of cyber incidents increases (Cyberattacks on the Rise as Confidence Sinks, Finds ‘2015 Cyberthreat Defense Report’ 2015), a threat arises not only to separate subjects but also to the country itself. Cyber attacks can be used as a means of political and economic pressure; in a serious crisis pressure can be exerted as an instrument of influence alongside traditional means of military force (Finlands`s Cyber Security Strategy 2013). Assurance of cybersecurity is a very important and specific type of activity that requires consistent and detailed legal regulation. Schjolberg and Ghernaouti-Hele consider cybersecurity to be a cornerstone of information society.

Lately increasingly more attention is given to cybersecurity on the regional level as well as in separate countries, including corresponding legal regulation, and the Republic of Lithuania is not an exception. Some of the main documents in this area are strategic documents, cybersecurity strategies (Mitrakas A. 2006). A national cyber security strategy is a tool to improve the security and resilience of national infrastructures and services (National Cyber Security Strategies 2012).

On 7 February 2013 the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy published a cybersecurity strategy (hereinafter – the Cybersecurity Strategy) together with a Commission proposed directive on network and information security. Article 5 of the Commission proposed directive on network and information security advocates for a national cybersecurity strategy in every country (Proposal for a Directive of European parliament and the Council concerning measures to ensure a high common level of network and information security across the Union 2013). In recent years strategic documents in the area of cybersecurity have been or are being adopted in some countries (Štitilis 2013).

Also legal regulation of cybersecurity is very important on the level of legal framework / laws. The importance of a law as such is unquestionable because it sets primary general rules that hold a specific legal power (Ragauskas 2005). The existence of rules of such nature is very important in a country, and their influence is very big. For example, the Federal Information Security Management Act of the USA recognizes the importance of information security to the economics and national security. In this context as new (cyber) threats arise and grow laws that regulate cybersecurity are passed in some countries, although this process is only starting.

Lithuania has also passed several strategic legal acts for cybersecurity assurance (Resolutions of the Government: on the approval of the programme for the development of electronic information security (cybersecurity) for 2011–2019 ("Regarding Approval of Electronic Information Security (Cyber Security) Development Programme for 2011–2019" 2011) (hereinafter – the Lithuanian Strategy), on the approval of the conception of the law on electronic communication networks and information security of the Republic of Lithuania (Regarding Approval of Conception of the Law on Electronic Communications Networks and Information Security 2006), and others). And in December of 2014 the Law on Cybersecurity of the Republic of Lithuania for regulating corresponding relations on the level of legal framework was passed.

As we can see a lot of attention is given to legal regulation of cybersecurity in Lithuania. But these are only the first steps in regulating this important area in Lithuania. Nevertheless, it is important to assess legal norms that have been approved up till now. Therefore the aim of this article is to analyse and assess legal regulation of cybersecurity of the Republic of Lithuania by strategic acts and regulation on the level of laws in Lithuania. First of all, the task raised is to reveal the historical retrospective of regulation of cybersecurity in the Republic of Lithuania. The next task is related to the analysis of Lithuanian strategic legal acts in the area of cybersecurity (including also a comparative analysis with EU strategic cybersecurity documents), and the third task is to analyse and assess the Law on Cybersecurity of the Republic of Lithuania. When analysing and assessing legal regulation the main attention will be given to the cybersecurity model, the institutional system, and the area of application as well as to the implementation of strategic aims and tasks.

Several different methods were used for the research: the method of empirical analysis of legal documents was used for identifying the legal regulation of cybersecurity in force in Lithuania. Strategic legal acts and laws of the Republic of Lithuania were analysed. This method allows, after performing analysis of official documents, to accurately identify and describe the relevant relationship among the existing legal regulation. When analysing strategic legal acts on cybersecurity assurance of Lithuania and the EU, the authors used the method of comparison. When using references to academic literature, the authors used the method of deduction, allowing to draw sufficiently reliable conclusions.

2. Historical retrospective of legal regulation of cybersecurity in Lithuania

Each state may have number of laws and regulations that effect the use of computer technology (Whitman, et al. 2014). In this part of the article we will review the strategic legal acts of the Republic of Lithuania in the area of cybersecurity, and how the corresponding legal regulation changed in Lithuania with passing years.

The need for strategic legal regulation of cybersecurity in Lithuania appeared in 2001 when, on 22 December 2001, the Government of the Republic of Lithuania passed the Resolution No. 1625 "On the Approval of State Strategy for Information Technology Security and Its Implementation Plan" ("Regarding Approval of State Strategy for Information Technology Security and Its Implementation Plan" 2001) (hereinafter – the 2001 Strategy). This resolution established the first national strategy of security of information technologies, but the term *cybersecurity* was still not used at that time. But the main aim of this Strategy was to regulate security only in public institutions, and security of information technologies in the private sector was not regulated. Having in mind that most often 85-90% of the cyber infrastructure is managed by the private sector (Rosenzweig 2013), also from the point of view of current legal regulation, it is possible to state that at that moment an essential mistake was made by not seeking to regulate IT security in the private sector. This gap of legal regulation in Lithuania was corrected only much later.

When analysing advanced aims of the 2001 Strategy it may be seen that one of the main aims was the development of legal regulation of information technology security. Points 1.1.–1.8. define areas of information technology security that should be regulated; point 1.8. foresees the introduction of a post of a data security representative. So there was already a need of function distribution at that time. Also attention should be given to the fact that not a lot of attention was given in the 2001 Strategy to the institutional regulation model because three institutions were mentioned in the 2001 Strategy as being responsible for information technology security or its implementation but only in the public sector. This may be explained by the fact that the view at the time on cyber threats was inadequate. These drawbacks were corrected a lot later when the attitude towards cyber threats changed.

On 19 June 2006 the Government of the Republic of Lithuania adopted the Resolution No. 601 "Electronic Information Security Strategy in State Information Systems till 2008" (hereinafter – the 2006 Strategy) ("Regarding Approval of Electronic Information Security Strategy in State Information Systems till 2008" 2006). Again it can be clearly seen that this 2006 Strategy was also meant only for regulation of electronic information security[1] in the public sector. Here, like in the 2001 Strategy, institutions responsible for implementing the strategy were appointed. When comparing with the previous strategy the institutional model is applied a lot more widely, 7 institutions responsible for the implementation of the measures foreseen in the 2006 Strategy are appointed, but again only in the public sector. Besides, functions of the institutions were not clearly distinguished, especially in the context of policy formation and implementation – the responsible institutions were indicated only as responsible performers of the plan of measures. The main institution in Lithuania in the area of electronic information security was also not named.

When analysing the aims of the 2006 Strategy it can be seen that one of the main extended tasks is to adopt legal acts that would regulate electronic information security – but again only in the public sector. So it is possible to state that the development of the regulation of electronic information security was foreseen in all programmes, because, with the development of information technologies, legal regulation and its improvement were necessary. But improvement of legal regulation was related only to the public sector. Also one of the extended tasks was to ensure the coordination of electronic information security.

Attention should be given to the fact that the 2006 Strategy performed an analysis of law-making implementing the State Strategy for Information Technology Security, adopted by Resolution No. 1625 of the Government of the Republic of Lithuania of 22 December 2001. During the period of 2002-2004, implementing the State Strategy for Information Technology Security, legal acts for regulation of information technology security were

[1] As we see, another term is used in the strategic document – not „information technology safety", but „electronic information safety".

passed, security of information systems was evaluated, more than 30 provisions on information systems' data security were coordinated with the Ministry of the Interior and approved, the organisation of training of security representatives was started, a department to coordinate information technology security in public institutions was established at the Ministry of the Interior ("Regarding Approval of Electronic Information Security Strategy in State Information Systems till 2008" 2006), but it may be seen that the tasks set by the 2001 Strategy on legal regulation were implemented only partially, identification of security requirements of electronic signature for personal identification and identification of responsibility according to the nature of violations were not regulated.

Apart from the 2006 Strategy another very important legal act was passed in 2006. On 6 December 2006 with the Resolution No. 1211 the Government of the Republic of Lithuania approved the concept of the law on electronic communication networks and information security of the Republic of Lithuania (hereinafter – the concept). This concept had to be the basis for the new law in the area of electronic communication networks and information security in Lithuania[2]. The concept provided that the law on electronic communication networks and information security of the Republic of Lithuania would regulate relations with electronic communication networks and information security (hereinafter – network and information security), would create conditions for the development of a secure information society, would increase the trust of consumers in information society („Regarding Approval of Conception of the Law on Electronic Communications Networks and Information Security" 2006). The main aim of the law according to the concept was supposed to be such: to define and embed the basis for legal regulation of public relations related to network and information security. The law was also supposed to fill the legal regulation gaps related to the provision of electronic communication services, as much as it is related to network and information security when providing electronic communication services.

After the approval of this concept a draft of the law on electronic communication networks and information security of the Republic of Lithuania was started to be prepared. A work group to prepare this draft law was created. The work group prepared a draft of the law but the law was never passed. According to the draft the law had to regulate public relations connected with electronic communication networks and information security, determining the general requirements for ensuring security of electronic communication networks and information as well as public relations connected with assessment of audit and technical and software security of electronic communication networks and information security of state and local governance institutions. This draft law already foresaw an institutional structure responsible for security of electronic communication networks and information in Lithuania. But the mentioned draft did not emphasize security of electronic communication networks and information of critical information infrastructures (Štitilis 2013), and it did not foresee a main institution responsible for the corresponding area in Lithuania[3].

So the first law for systematic regulation of cybersecurity in Lithuania could have been passed already in 2006-2007 but it wasn't. The Law on Cybersecurity was passed only in 2014. Although from 2006-2007 till 2014 there were no cyber incidents that would have had a significant impact on critical information structures[4] in Lithuania, nevertheless certain cyber incidents were recorded. One of the biggest attacks in Lithuania was the attack against the news portal *Delfi* in May of 2013, when the number of queries in several minutes reached 50 million, data stream was 6 gigabits per second. The equipment was working under critical limits, and customer service was upset ("Lithuania - cyber war in the trenches" 2014). Also on 27 January 2012 there was a cyberattack of the DDoS type (*Distributed denial-of-service*) at the Lithuanian Bank. These attacks demonstrated how important it was to identify critical information infrastructure in a country in order to protect it appropriately.

Also it should be mentioned that without a basic cybersecurity legal regulation the cybersecurity culture in

[2] As we see, additional term is used – „electronic communication networks and information security". This term is in its essence perhaps most associated with the term „Cybersecurity".

[3] As indicated in the Law on Cyber Security of the Republic of Lithuania from January 1, 2015 (National Cybersecurity Centre).

[4] However, there is no such infrastructure identified in Lithunia yet.

Lithuania was forming very weakly. That means that at the moment after the passing of the Law on Cybersecurity this area is only in the initial development stage.

Apart from the adopted legal acts the year 2006 was also important because, as part of the implementation of the Resolution No. 315 of the Government of the Republic of Lithuania of 24 March 2005 "On Approval of Lithuanian Government Programme Implementation Measures for 2004-2008" („Regarding Approval of Lithuanian Government Programme Implementation Measures for 2004–2008" 2005), the Computer Emergency Response Team (hereinafter – CERT) was established at the Communications Regulatory Authority of the Republic of Lithuania on 2 October 2006. But this CERT department works only with incidents in electronic communication networks, in other words, it receives information about incidents only from Internet service providers. There are doubts if such activity of CERT is of real value. According to the authors, establishment of a national CERT would help to more effectively ensure cybersecurity not only in the area of electronic communications but also in other related areas of cybersecurity including critical information infrastructures of corresponding sectors. According to the authors, in order to efficiently ensure cybersecurity in Lithuania it is necessary to clearly distribute, purify, and centralise the functions of CERT.

Summarizing this part several main problems encountered when seeking to regulate cybersecurity may be distinguished:
- Legal regulation of cybersecurity in Lithuania was initiated and performed quite passively although it was foreseen as one of the priorities in the 2001 and 2006 Strategies.
- These programmes talked about legal regulation of cybersecurity only for state institutions, and the private sector was completely forgotten.
- The 2001 and 2006 Strategies aimed to create cybersecurity coordination, to appoint institutions responsible for cybersecurity, and to separate functions of the mentioned institutions, but in fact it all went on until 2014 when the Law on Cybersecurity was passed, and until then legal regulation was intermittent and not thorough.

Currently according to the legal acts in force the division of CERT in Lithuania exists as a component of the Communications Regulatory Authority of the Republic of Lithuania and works only with incidents in electronic communication networks. Doubts arise if such activities of CERT are of real value. Establishment of a national CERT would help to more effectively ensure cybersecurity not only in the area of electronic communications. Seeking to ensure cybersecurity effectively it is necessary to clearly distribute, purify, and centralize the functions of CERT.

- In the 2001 Strategy not a lot of attention was given to the institutional regulation model because only three institutions were mentioned as responsible for cybersecurity or its implementation in this Strategy; 7 institutions were mentioned as responsible for implementation of the planned measures in the 2006 Strategy, but one main institutions was not named in the 2006 Strategy. So when comparing with the previous strategy it may be seen that the institutional model is applied much more widely, but functions of certain institutions are not detailed especially from the aspect of policy formation and implementation.

3. Strategic legal regulation: strategies of Lithuania and the European Union

This part will analyse the Lithuanian Strategy and will compare it with the cybersecurity strategy of the European Union (hereinafter – the EU Strategy). The Lithuanian Strategy currently in force was approved on 29 June 2011. This Lithuanian Strategy names the main problems of electronic information security (cybersecurity) and set the aims and tasks of development of electronic information security (cybersecurity) ("Regarding Approval of Electronic Information Security (Cyber Security) Development Programme for 2011–2019" 2011). It is necessary to add that the Lithuanian Strategy is the first cybersecurity strategy that foresees not only regulation of the sector of cybersecurity of state institutions but also regulation of the private and personal sector.

First of all, attention should be given to the fact that the Lithuanian Strategy uses two concepts that are treated as synonyms although essentially they are different:

- Electronic information security is ensuring confidentiality, integrity, and accessibility of electronic information (Ministry of the Interior, Electronic Information security, 2015).
- Cybersecurity is a totality of legal, information dissemination, organisational and technical means meant to avoid, find, analyse, and react to cyber incidents, also for restoring the usual activities of management systems of electronic communication networks, information systems or industrial processes after such incidents (Law on Cyber Security of the Republic of Lithuania 2015).

According to the definitions of the concepts it may be seen that electronic information security is a narrower concept encompassing the general features of security but that does not distinguish the measures, incident management, etc. According to the definitions of the concepts it is possible to state that electronic information security is a component of cybersecurity therefore a uniform and wider concept should be used in legal acts that corresponds to the current complex assurance of infrastructure security.

Point 2 of the Lithuanian Strategy identifies a quite specific and ambitious strategic aim that should be reached in 2019: to develop electronic information security in Lithuania, to ensure cybersecurity and to reach that in 2019 the part of state information resources that corresponds to electronic information security (cybersecurity) requirements determined by legal acts would reach 98% of all state information resources, that the average time for liquidating critical information infrastructure incidents would decrease to 0.5 hour, and that the percentage of Lithuanian inhabitants, who feel safe in cyberspace, would reach 60%.

The EU Strategy starts with the following concept "An Open, Safe and Secure Cyberspace" – that is a thorough EU vision how to best prevent disruption of cyber activities and attacks and what responsive measures should be taken. It seeks to promote European values of freedom and democracy and to ensure secure development of digital economy. Specific actions are meant for increasing resistance of information systems to cybercrimes and for strengthening EU international cybersecurity policy and cyber defence (Štitilis D. 2013). Similarly as in the Lithuanian Strategy the main aim of the Strategy is foreseen – which is the assurance of the security of an open and reliable cyberspace, but implementation of the aims of the EU Strategy is not related to percentage numbers of people, who feel safe in cyberspace, which remind of high-sounding slogans because up till now no such research has been performed and the starting point to measure the increasing or decreasing security of the society in cyberspace is not known.

When assessing the provisions stated in points 6-10 of the Lithuanian Strategy it is possible to state that the following main aims and tasks to be reached are determined there:
- To reach that the security of state information resources is ensured. The following tasks are foreseen to reach this aim: to improve coordination and maintenance of electronic information security (cybersecurity); to improve legal regulation of electronic information security (cybersecurity); to widen and develop safe state information infrastructure; to promote implementation of projects of electronic information security (cybersecurity); to develop international cooperation in the area of electronic information security (cybersecurity).
- To ensure efficient functioning of critical information infrastructure. The following task is foreseen to reach this aim: to ensure security of critical information infrastructure.
- To seek to ensure security of Lithuanian inhabitants and people present in Lithuania in cyberspace. The following tasks are foreseen to reach this aim: to raise the culture of electronic information security (cybersecurity); to strengthen the security of the Lithuanian cyberspace; to ensure the protection of the virtual perimeter of the Lithuanian cyberspace from external cyberattacks; to strengthen the security of services provided in cyberspace.

Five strategic priorities are emphasized in the EU Strategy („Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace" 2013):
1. Achieving cyber resilience;
2. Drastically reducing cybercrime;
3. Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy;
4. Develop the industrial and technological resources for cybersecurity;

5. Establish a coherent international cyberspace policy for the European Union and promote core EU values.

When comparing the main priorities of the EU Strategy with the Lithuanian Strategy many similar and priority measures may be seen, although the Lithuanian Strategy was adopted almost 2 years earlier, but attention should be given to the fact that the measures defined in the Lithuanian Strategy are difficult to implement or immeasurable. For example, the annex of the Lithuanian Strategy, next to the sought aims and tasks, identifies the assessment criteria for strategy implementation, their sought values for 2011, 2015 and 2019, and institutions responsible for implementation of these criteria. Specific and ambitious values of assessment criteria are identified, but it is not clear if they can be really implemented because many indicators were never assessed before the adoption of the Lithuanian Strategy: e.g., it is foreseen that the part of information resources that uses secure state infrastructure will reach 70% by 2015 and 100% by 2019, although it is not known what the value of this index was in 2011. According to the authors, with regard to the fact that values of many assessment criteria are unknown, the Lithuanian Strategy had to indicate that the first assessment should be performed a lot earlier than in 2015, seeking to identify the primary values of corresponding indices (i.e., to assess the current situation), and afterwards it would be possible to determine the values that need to be reached in the coming years.

Besides, according to the authors, it might be difficult to precisely assess some indicators, e.g., it is indicated that the part of Lithuanian inhabitants, who feel safe in cyberspace, should reach 40% in 2015 and 60% in 2019. The feeling of social security should be assessed by social research but thorough research in Lithuania in this area has never been performed, except for the research on identity theft (Štitilis *et al*. 2011).

Point 1.2 of the Lithuanian Strategy also foresees the task "to improve legal regulation of electronic information security (cybersecurity)", for the implementation of which five criteria are foreseen, according to which it would be possible to judge successful implementation of the strategy:
- the part of passed or changed legal acts from the legal acts which need to be passed or changed, in percentage;
- special laws, determining essential requirements related to ensuring electronic information security (cybersecurity), that regulate specific activity and legal relations (the Law on Electronic Communication Networks and Information Security of the Republic of Lithuania among them) are passed;
- the part of passed or changed law implementing legal acts from the legal acts which need to be passed or changed, in percentage;
- requirements for the provisions of services of a secure state data transmission network are approved;
- classification of identification measures (methods) and service reliability (coordinated with that of other Member States of the European Union), technical and procedural requirements, the order of accreditation and use are approved.

When analysing these criteria, e.g., 1 and 3, it seems that these criteria can be implemented only formally, because we did not succeed in finding statistics on the need of legal acts that need to be changed related to cybersecurity in the public space, therefore a conclusion may be made that institutions responsible for the changing of such legal acts can implement these task formally only because that after the passing of the Law on Cybersecurity a natural legal need to change legal acts related to cybersecurity appeared with the appearance of additional legal regulation.

The EU Strategy clearly foresees institutions responsible for cybersecurity on the national as well as EU level. It is shown in Fig 1.

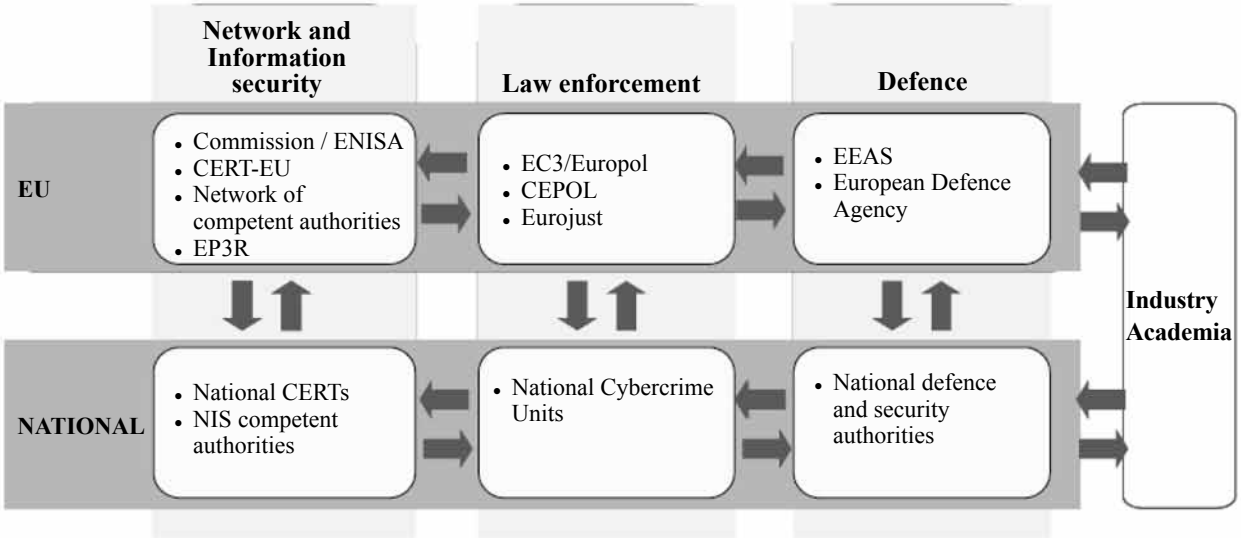

Fig 1. Institutions responsible for cybersecurity.

Source: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions "Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace", JOIN/2013/1 final. Brussels, 2013.

There was a lack of such clear distribution of responsibility and functions in the Lithuanian Strategy because institutions responsible for implementation of certain measures for reaching certain aims were foreseen in it, but specific functions were not defined. When comparing the provisions of the EU and the Lithuanian Strategies it may be seen that the aims are common, they do not distort or contradict the principles of cybersecurity regulation of EU and Lithuanian law.

It is necessary to mention that in the context of the EU and Lithuanian Strategies it is possible to see three main aims:
- protection of information society;
- ensuring cybersecurity in the public and private sectors;
- fight with criminal offences in cyberspace.

So it is possible to state that priorities of the strategies are uniform, and the objective is common, but the implementing means of the Lithuanian Strategy to reach these aims are not always real or sometimes only formal, differently from the EU Strategy.

Summarizing this part it is possible to state that the main priority purposes and the common objective of the Lithuanian and the EU Strategies are the same, but there is no clear distribution of functions for responsible institutions in the Lithuanian Strategy, some tasks cannot be implemented or can be implemented only formally. The chosen criteria are not clear because there are no specifically identified research-based starting points that could be used to assess timely and efficient implementation of the Lithuanian Strategy. When analysing the measures foreseen in the EU Strategy it is possible to state that the legal regulation of the Republic of Lithuania corresponds to that of the EU because it implements the measures foreseen in the EU Strategy. Priorities of the EU and the Lithuanian Strategies are uniform but the implementation measures of the Lithuanian Strategy are not always real or only formal.

4. Analysis of the Law on Cybersecurity of the Republic of Lithuania

This part of the article will analyse the provisions of the Law on Cybersecurity and will try to assess if the Law on Cybersecurity will help to implement the aims and tasks foreseen in the Lithuanian Strategy, if the legal regulation gaps were filled after the passing of this Law. Also the Law on Cybersecurity will be assessed in the

context of EU strategic legal regulation.

As mentioned above, on 11 December 2014 the Seimas of the Republic of Lithuania adopted the Law on Cybersecurity of the Republic of Lithuania (Law on Cyber Security of the Republic of Lithuania 2015). It was an especially important event for Lithuania although the concept was approved on 6 December 2006 by the Resolution No. 1211 of the Government of the Republic of Lithuania. It is necessary to draw attention that the Law on Cybersecurity was passed practically without a relevant concept because the concept of 2006 was morally obsolete during the discussion of the Law on Cybersecurity. The concept adopted 9 years ago did not reflect the current situation of cybersecurity as information and communication technologies were quickly marching ahead, the National Cybersecurity Centre, established almost without any basis, was not foreseen in it. The adoption of the Law on Cybersecurity without a basis that corresponds to realities of the present is not a good initiative being the reason why gaps in the law may become apparent in the future that may have a negative impact on cybersecurity in Lithuania.

The Law on Cybersecurity that is currently in force consists of 5 chapters: general provisions, institutions, responsible for policy formation in the area of cybersecurity, responsibilities of participants of cybersecurity, basis for inter-institutional cooperation, exchanging of information and responsibility, and final provisions.

Part 1 of Article 1 of the Law on Cybersecurity determines institutions that form and implement cybersecurity policy, their competencies, functions, rights and obligations, obligations and responsibility of managers and (or) processors of state information resources, managers of critical information infrastructure, public communication networks and (or) public electronic communication service providers and electronic information hosting service providers and measures of ensuring cybersecurity (Law on Cyber Security of the Republic of Lithuania 2015). The Law distributes the limits of responsibilities of the public sector institutions for cybersecurity quite consistently and clearly. Also it is important that the Law on Cybersecurity is applied not only to the public but also to the private sector, obligations are foreseen separately not only for electronic communication service providers but also for hosting service providers, and, most importantly, the Law foresees critical information infrastructure, a big part of which is managed by the private sector.[5]

According to the authors, critical information infrastructure protection is especially important seeking to avoid consequences destabilizing infrastructures after cyberattacks or incidents of other nature. A more detailed regulation of critical information infrastructure will be consolidated in accompanying legislation.

Part 1 of Article 4 of the Law on Cybersecurity foresees that strategic aims of cybersecurity policy and measures necessary to reach them are set by the Government of the Republic of Lithuania. So it is possible to state that the Government is the main institution that formulates strategic policy in the area of cybersecurity.

Part 2 of Article 4 of the Law on Cybersecurity foresees institutions responsible for cybersecurity, shown in Fig 2.

[5] According to article 2 part 2 of the Law, Critical information infrastructure shall mean an electronic communications network or a part of such a network, an information system or a part of such a system, a group of information systems or an industrial process control system or a part of such a system, regardless of whether it is managed by a private or public administration entity, where an incident occurring in any of the above may cause serious damage to the national security, the country's economy, national and public interests.

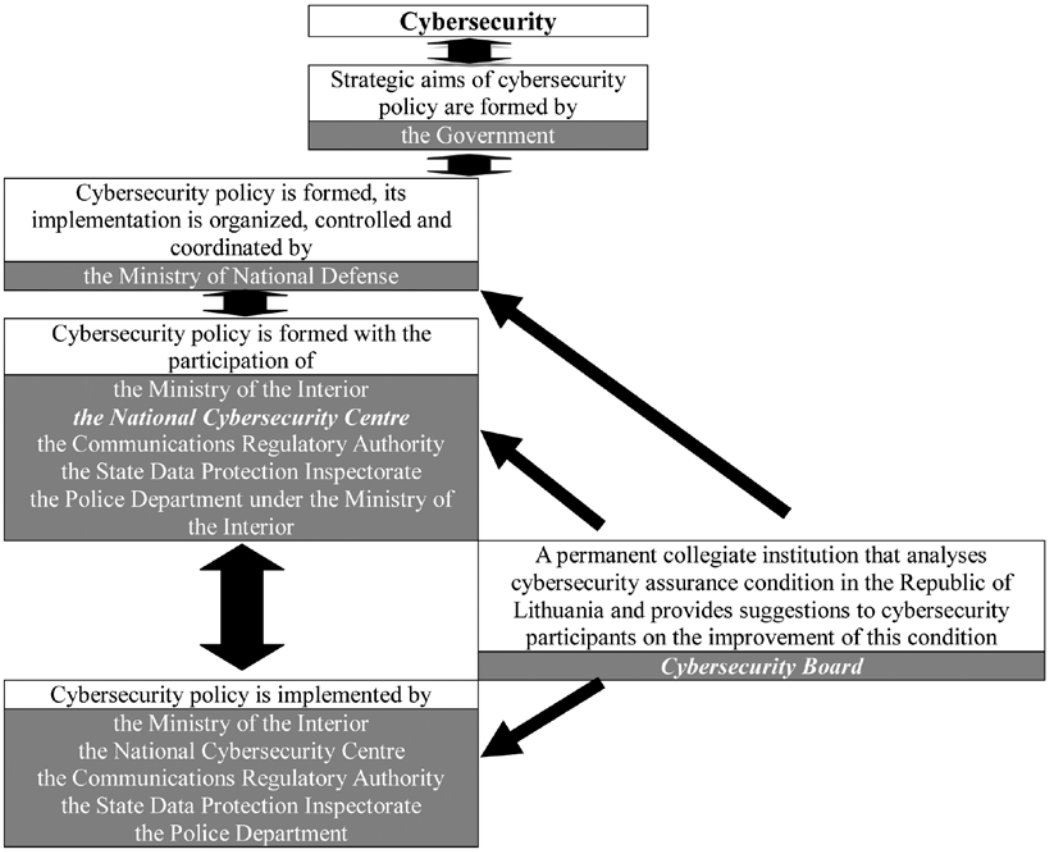

Fig 2. State institutions responsible for cybersecurity

Compiled by the authors.

As we can see according to the presented diagram this part of the law clearly distinguishes public institutions responsible for cybersecurity in Lithuania and the implementation of the provisions of the Law. The presented diagram shows the role of responsible institutions in the area of cybersecurity, but there are quite many responsible institutions, and functions of the institutions that form cybersecurity policy and perform control functions have not been detailed and specified. Also the national Computer Emergency Response Team CERT is not foreseen in the Law on Cybersecurity because, as mentioned, at the moment CERT is under the Communications Regulatory Authority. It is not clear if such department and its subordination should remain in the future or if the CERT, which is a part of the Communications Regulatory Authority, should be joined to the National CERT Department when such is established in the future.

Although the EU Strategy mentions aspects of cyber defence and resistance, cyber defence and its basics are not regulated in the Law on Cybersecurity of the Republic of Lithuania. Elements of cyber defence in Lithuania will most certainly be determined in the accompanying legislation; nevertheless, the basics of this defence should be consolidated on the level of a law.

More detailed legal regulation of certain narrow areas is also missing, e.g., point 3.1. of the Lithuanian Strategy foresees the task to "raise the culture of electronic information security (cybersecurity)", which can be reached, in our opinion, by educating the information society, raising consumer culture, etc., but this is mentioned in the Law on Cybersecurity only in point 9 of Part 2 of Article 10, in the functions of the National Cybersecurity Centre: "performs dissemination of information related to cybersecurity" (Law on Cyber Security of the Republic of Lithuania 2015). Several institutions were responsible for implementation of this task in the Lithuanian Strategy: the Ministry of the Interior, the Communications Regulatory Authority, the Ministry of Education and Science, the State Data Protection Inspectorate, but the Ministry of Education and Science is not even

mentioned in the Law on Cybersecurity. It is clear that when seeking to educate the society on the questions of cybersecurity it is necessary to create continuous publicity programmes so that the society would be constantly informed on the subject of cybersecurity. Education should be a continuous process as well as the development of the legal basis for cybersecurity; therefore more detailed regulation of this area is called for. The law should establish the main legal norms on public education in the area of cybersecurity.

Implementing the provisions of the Law on Cybersecurity, the National Cybersecurity Centre at the Ministry of National Defence was established on 1 January 2015 (hereinafter – the Centre) with the aim to analyse the national cybersecurity situation, to prepare reports on the condition of cybersecurity, to provide consultations and recommendations on cybersecurity and to ensure cybersecurity of state information resources during cyber incidents (National Cyber Security Center, 2015). Such centre was not mentioned neither in the Lithuanian Strategy nor in the Concept but its necessity for the assurance of Lithuanian cybersecurity is unquestionable.

Summarizing it is possible to state that the Law on Cybersecurity formally filled some gaps of the Lithuanian national legal regulation in the area of cybersecurity, but more detailed regulation of certain narrow areas is missing. The provisions of the Law regulate the functions of the Government and state institutions responsible for cybersecurity, but the institutional structure of the law is not perfect, there are quite many responsible institutions, and functions of the institutions that form cybersecurity policy and perform control functions have not been described in detail. Also the national Computer Emergency Response Team CERT is not foreseen in the Law on Cybersecurity because currently a functioning CERT is a part of the Communications Regulatory Authority. Also attention should be given to the fact that the Law on Cybersecurity does not talk about public education, which is very important seeking for cybersecurity. It is necessary to mention additionally that the Law on Cybersecurity does not foresee any basics for cyber defence; it does not mention any requirements for equipment manufacturers, which are very important. Also a lot of attention is given in the Law to critical information infrastructure protection, which is very important seeking to avoid outcomes destabilizing infrastructures after cyberattacks or incidents of another nature.

5. Conclusions:

When analysing legal regulation of cybersecurity it is possible to point out several main problems encountered when seeking to regulate cybersecurity:

Legal regulation of cybersecurity in Lithuania was initiated and performed quite passively although it was foreseen as one of the priorities in the 2001 and 2006 Strategies.

These programmes sought to establish legal regulation of cybersecurity only for public institutions, and the private or personal sector was completely forgotten.

The 2001 and 2006 Strategies sought to create coordination of cybersecurity, to appoint institutions responsible for cybersecurity, and to distinguish functions of the mentioned institutions, but in reality it took until 2014 when the Law on Cybersecurity was passed – before that legal regulation was intermittent and incomplete.

CERT works with incidents in electronic communication networks. Doubts arise if such activities of CERT are of full value? In our opinion the establishment of a national CERT would help to ensure cybersecurity more efficiently not only in the area of electronic communications. When seeking to effectively ensure cybersecurity it is necessary to clearly distribute, purify, and centralise functions, giving the technical functions of ensuring cybersecurity to the national CERT.

The 2001 Strategy did not give much attention to the institutional regulation model because only three institutions were mentioned in the 2001 Strategy as responsible for cybersecurity and its implementation. There were 7 institutions responsible for the implementation of the foreseen measures in the 2006 Strategy, but this strategy also did not appoint one institution that would be specifically responsible for cybersecurity. So, when

comparing with the previous Strategy, it may be seen that the institutional model is applied a lot more widely but functions of specific institutions are not described in detail.

The main priority purposes and the common objective of the Lithuanian Strategy and the EU Strategy are the same but there is no clear division of functions for responsible institutions in the Lithuanian Strategy, and some tasks cannot be implemented or can be implemented only formally. The chosen criteria are not clear because there are no specifically identified research-based starting points that could be used to assess timely and efficient implementation of the Lithuanian Strategy. When analysing the measures foreseen in the EU Strategy it is possible to state that legal regulation of the Republic of Lithuania does not formally fall behind the EU regulation because it implements the measures foreseen in the EU Strategy. Lithuania has an already adopted Law on Cybersecurity in force since 2015 that distributes functions to the institutions responsible for cybersecurity. Priorities of the EU and Lithuanian Strategies are the same, but the implementing measures foreseen in the Lithuanian Strategy are not always real or only formal.

The Law on Cybersecurity formally filled some gaps of the Lithuanian legal regulation in the area of cybersecurity, but more detailed regulation of certain narrow areas is missing. The provisions of the Law regulate the functions of the Government and state institutions responsible for cybersecurity, but institutional structure of the law is not perfect, there are quite many responsible institutions, and functions of the institutions that form cybersecurity policy and perform control functions have not been described in detail. Also the national Computer Emergency Response Team CERT is not foreseen in the Law on Cybersecurity because currently a functioning CERT is a part of the Communications Regulatory Authority.

Also attention should be given to the fact that the Law on Cybersecurity does not talk about public education, which is very important seeking for cybersecurity. It is necessary to mention additionally that the Law on Cybersecurity does not foresee any basics for cyber defence. A positive feature is that a lot of attention is given in the Law to critical information infrastructure protection, which is very important seeking to avoid outcomes destabilizing infrastructures after cyberattacks or incidents of another nature.

References

Cyberattacks on the Rise as Confidence Sinks, Finds '2015 Cyberthreat Defense Report'. 2015. Available on the Internet: <http://www.businesswire.com/news/home/20150311005119/en/Cyberattacks-Rise-Confidence-Sinks-Finds-%E2%80%982015-Cyberthreat#.VRWGp3mKCM8>

Finlands`s Cyber Security Strategy. Government Resolution 24.1.2013. Forssa print, 2013, 1. ISBN 978-951-25-2438-9.

Grubicka, J.; Matuska, E. 2015. Sustainable entrepreneurship in conditions of UN (Safety) and technological convergence, *Entrepreneurship and Sustainability Issues*2(4):188–197. DOI: http://dx.doi.org/10.9770/jesi.2015.2.4(2)

Joint Communication to the European Parliament, the Council, the European Ecomonic and Social Committee and the Committee of Regions „Cybersecurity strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN/2013/1 final. Briussels, 2013. Available on the Internet: <http://ec.europa.eu/ information_society/newsroom/cf/dae/document.cfm?doc_id=1667>

Krašto apsaugos ministerija Nacionalinios kibernetinio saugumo centras [Ministry of National Defence, National Cyber Security Center], 2015. Available on the Internet: <http://www.kam.lt/lt/struktura_ir_kontaktai_563/kas_institucijos_567/rysiu_ir_informaciniu_sistemu_tarnyba_prie_kam_2482/nacionalinis_kibernetinio_saugumo_centras.html>

Lankauskienė, T.; Tvaronavičienė, M. 2012. Security and sustainable development approaches and dimensions inn the globalization context, *Journal of Security and Sustainability Issues* 1(4): 287-297. http://dx.doi.org/10.9770/jssi.2012.1.4(5)

Lietuvos Respublikos kibernetinio saugumo įstatymas [Law on Cyber Security of the Republic of Lithuania] 2014. Available on the Internet: <https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4>

Lietuvos Respublikos Vyriausybės 2001 m. gruodžio 22 d. nutarimas Nr. 1625 „Dėl Informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo" [Resolution of the Government of the Republic of Lithuania of December 22, 2001 No. 1625 „Regarding Approval of State Strategy for Information Technology Security and Its Implementation Plan"].Available on the Internet: <https://www.e- tar.lt/portal/lt/legalAct/TAR.842ABCDE6836>

Lietuvos Respublikos vyriausybės 2005 m. kovo 24 d. nutarimas Nr. 315 „Dėl Lietuvos Respublikos Vyriausybės 2004–2008 metų programos įgyvendinimo priemonių patvirtinimo“ [Resolution of the Government of the Republic of Lithuania of March 24, 2005 No. 315 „Regarding Approval of Lithuanian Government Programme Implementation Measures for 2004–2008]. Available on the Internet: <http://www3.lrs.lt/pls/inter2/dokpaieska.showdoc_l?p_id=279570>

Lietuvos Respublikos Vyriausybės 2006 m. birželio 19 d. nutarimas Nr. 601 patvirtino „Elektroninės informacijos saugos valstybės institucijų informacinėse sistemose valstybinę strategiją iki 2008“ [Resolution of the Government of the Republic of Lithuania of June 19, 2006 No. 601 „Regarding Approval of Electronic Information Security Strategy in State Information Systems till 2008“]. Available on the Internet: <https://www.e-tar.lt/portal/lt/legalAct/TAR.6C6C30A92607>

Lietuvos Respublikos Vyriausybės 2006 m. gruodžio 6 d. nutarimas Nr. 1211 „Dėl Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcijos patvirtinimo“ [Resolution of the Government of the Republic of Lithuania of December 6, 2006 No. 1211 „Regarding Approval of Conception of the Law on Electronic Communications Networks and Information Security“]. Available on the Internet: <https://www.e-tar.lt/acc/legalAct.html?documentId=TAR.522926ED3AA1>

Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 “Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo”; 2011, Nr.106 (atitaisymas) [Resolution of the Government of the Republic of Lithuania of June 29, 2011 No. 796 “Regarding Approval of Electronic Information Security (Cyber Security) Development Programme for 2011–2019”; 2011, No.106 (correction)]. Available on the Internet: <https://www.e-tar.lt/portal/lt/legalAct/TAR.1ABB945646B7>

Lietuvos žinios, Lietuva kibernetinio karo apkasuose [Newspaper Lithuanian news, Lithuania - cyber war in the trenches], 2014. Available on the Internet: <http://lzinios.lt/lzinios/Lietuvoje/lietuva-kibernetinio-karo-apkasuose/187968>

Mitrakas A. 2006. Information Security Law in Europe: Risks Checked. *Information & Communications Technology Law* 15(1), DOI: http://dx.doi.org/10.1080/13600830600557984

National Cyber Security Strategies. Setting the source for national efforts to strengthen security in cyberspace. European Network and Information Security Agency (ENISA), 2012; p. 4. DOI: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport

Proposal for a Directive of European parliament and the Council concerning measures to ensure a high common level of network and information security across the Union, COM/2013/48 final. Briuselis, 2013. Available on the Internet: <http://ec.europa.eu/information_society/newsroom/cf/dae/document. cfm?doc_id=1666>

Ragauskas P. 2005. Įstatymo samprata [Conception of Law] // Jurispriudencija [Jurisprudence], 67(59).

Rosenzweig, P. 2013. Cyber warfare: how conflicts in cyberspace are challenging America and changing the world. – library of Congress Cataloging, ISBN – 9780313398957.

Stańczyk, J. 2011. European security and sustainability issues in the context of current international environment, *of Security and Sustainability Issues* 1(2): 81–90.http://dx.doi.org/10.9770/jssi.2011.1.2(1)

Štitilis D. [et al.] 2011. Tapatybės vagystė elektroninėje erdvėje, socialiniai elektroninio verslo ir teisinio reguliavimo aspektai [Identity Theft in Cyberspace: Social, Electronic Business and Legal Regulation] Issues. – Mykolo Romerio universitetas [Mykolas Romeris University].

Štitilis D. 2013. Legal Regulation of Cybersecurity: Cybersecurity Strategies // Social Technologies, 3(1), DOI: http://dx.doi.org/10.13165/ST-13-3-1-13

Vidaus reikalų ministerija, Elektroninės informacijos sauga [Ministry of the Interior, Electronic Information security], 2015. Available on the Internet: <http://www.vrm.lt/e-sauga>

Vosylius, E.; Rakutis, V.; Tvaronavičienė, M.2013. Economic growth, sustainable development and energy security interrelation, *Journal of Security and Sustainability Issues* 2(3): 5–14.http://dx.doi.org/10.9770/jssi.2013.2.3(1)

Wahl, M. 2014. Sustainable Entrepreneurship: The Wolf ButterBack Case, *Entrepreneurship and Sustainability Issues* 1(4):223–229. DOI: http://dx.doi.org/10.9770/jesi.2014.1.4(4)

Wahl, M.; Prause, G. 2013. Toward understanding resources, competencies, and capabilities: business model generation approach, *Entrepreneurship and Sustainability Issues* 1(2): 67–80 http://dx.doi.org/10.9770/jesi.2013.1.2(1)

Whitman, M.E, Mattord, H.J. 2014. Management of Information Security, 4th Edition.