The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2016 Volume 4 Number 2 (December)

ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/

PRECONDITIONS OF SUSTAINABLE ECOSYSTEM: CYBER SECURITY POLICY AND STRATEGIES[1]

Darius Štitilis [1], Paulis Pakutinskas [2], Inga Malinauskaitė [3]

[1,2,3] Mykolas Romeris University, Ateities str.20, Vilnius, Lithuania

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

Received 17 May 2016; accepted 25 August 2016

Abstract. Ten years have already passed since the first cyber security strategies were drawn up in different countries reflecting global cyber security policy. The aim of this scientific article is to analyze the historical development of cyber security strategies of selected EU and NATO countries and to reveal future trends of cyber security policy. The article examines key elements of the selected strategies in the initial cyber security strategies and the description thereof in the already improved cyber security strategies. We selected countries with different allegiances. First, we chose two countries that are members of both the EU and NATO (the Netherlands and Estonia), then a country, which is only a member of NATO, namely, the United Stated of America, thirdly, an EU state, which is not a member of NATO, namely, Finland. We believe the research results may be used for both the development of current cyber security strategies, as well as well as for drafting a cyber security policy.
Keywords: cyber security strategy, historical development, entrepreneurship, policy

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

JEL Classifications: O33; D80

1. Introduction

More and more countries have become some kind of victims of cyber-attacks on the one hand, and have realized the seriousness of cyber-attacks and the importance of cybersecurity on the other hand (Ventre D., 2015; Allabouche, et al. 2016; Samašonok, et al. 2016; Belás, et al. 2016). The concept 'cyber security' emerged in the1990s, when the increasing dependence of the public on the development of information technologies was observed. Cyber security is associated with the creation and maintenance of processes related to the identification of emerging cyber threats and costs for the application of reasonable countermeasures (Shoemaker and Conklin, 2012). Cybersecurity is not an isolated objective, but rather a system of safeguards and responsibilities to ensure

[1] *This article is part of the research 'Analysis and adaptation of EU and NATO cyber security strategies: Lithuanian cyber security model', funded by the Research Council of Lithuania (Grant No. MIP-099/2015/PRC-36).*

the functioning of open and modern societies (Klimburg A., 2012), also it`s a precondition of sustainable ecosystem. The United States Computer Science and Telecommunications Board, which conducts scientific research in the field of cyber security each year, noted that cyber security is the main challenge of public policy (2015). Key components of cyber security are laid down in the main strategic documents, namely, cyber security strategies. In other words, cyber security strategies define and institutionalize the national cyber security system (Cezar, 2013).

The aim of this article is to reveal future insights into and tendencies of cyber security strategies. Origins of the cyber security regulatory initiatives may be associated with fragmented legal provisions in certain sectors. However, with the increase in cybercrime, the need to have new regulatory initiatives creating presumptions for a unified cyber security regulation has been growing. Documents in the cyber security area first appeared in the early 2000s. Russia adopted the National Security Concept of the Russian Federation in 2000; in 2003, the US passed the National Strategy to Secure Cyberspace; in 2005, Germany adopted a National plan for Information Infrastructure protection. It should be noted that for the most part these first documents were not yet referred to as cyber security strategies; they were more like plans, security strategies, information security strategies or strategies on critical infrastructures on the basis whereof countries later adopted cyber security strategies.

There has been a remarkable increase in the adoption of cyber security strategies since 2011. This was when most EU member states and other countries adopted cyber security strategies. For example, Luxembourg adopted its cyber security strategy in 2011, Georgia – in 2012, Italy – in 2013, and Denmark and Iceland – in 2014. Regional Cyber Security Strategy of the European Union approved in 2013 and Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union adopted in 2016. The objective of this Directive is to achieve a high common level of security of network and information systems in the Union while adopting minimum harmonisation requirements. It is noteworthy, that several countries have already adopted second versions of their cyber security strategies. The goal of this article is to research the historical development of the cyber security strategies of the selected European Union and NATO countries.

2. Methodology

Countries, whose cyber security strategies have demonstrated a significant change have been selected for the research. The research has been carried out by analyzing the content of the initial and second cyber security strategies of the selected countries. In particular we assessed constituent elements of cyber security strategies, such as threats and challenges, principles, methods, key goals and implementation. These particular elements were chosen because it was noted they were key composite elements of both initial and second strategies, and comprehensively disclose the content of cyber security strategies. The course of the research evaluates the change of constituent elements of strategies throughout their history, examines how the content of the selected cyber security strategies has changed over time, solves issues and proposes methods to address various questions.

Countries that are members of the European Union and NATO, as well as those that are members of NATO or the European Union alone, were chosen for the research analysis. First, countries belonging to both the European Union and NATO, namely, the Netherlands and Estonia were chosen. Then, for further comparison of the historical development of cyber security strategies, a country which is a member of NATO alone, namely, the USA, was selected. And finally an EU member state which is not a member of NATO, namely, Finland. These four countries have already adopted second cyber security strategies. This different level of participation by countries in international organizations is believed to be able to reveal trends of cyber security strategies, and also to reveal regional cyber security perspectives.

3. National Cyber Security Strategies of the Netherlands of 2011 and 2013

The Netherlands adopted its first cyber security strategy in 2011. The first part of the strategy contained the presentation of the issue, principles and goals of the cyber security policy. The second part of the strategy established specific actions, which the Government had to implement together with other cooperating authorities. The first strategy of the Netherlands formulated fundamental cyber security principles, such as promotion of public and private partnership, active international cooperation, allocation of responsibilities between ministries, etc. The aim of the strategy was security and confidence in an open and free digital society. The second part of the strategy enshrined a specific action plan, including but not limited to the establishment of a cyber security council and the national cyber security centre, assessment of threats and risks, enhancement of the protection of critical infrastructures, development of possibilities to repel potential attacks, investigation of cybercrime and promotion of research and education.

The second cyber security strategy of the Netherlands was adopted in 2013. It emphasized the correlation between security, freedom and socioeconomic benefits. One of the fundamental principles enshrined therein is that responsibilities applicable in physical space should also apply in cyber space. Thus, in order for a dialogue on cyber security between various stakeholder groups to reach a new level of maturity, three key elements should be considered: the development of self-regulation, transparency and awareness. The second strategy clearly allocates the responsibilities of different authorities, namely, it identifies areas of responsibility of the government, the business sector and individuals.

The historical development of the cyber security strategies of the Netherlands can obviously be characterized by a significant change in its constituent elements. This valuable change of elements is reflected in a comparative table of key constituent elements of the cyber security strategies:

Table 1. Comparison of strategies

National Cyber Security Strategy of the Netherlands of 2011	**National Cyber Security Strategy of the Netherlands of 2013**
Partnership between public and private sectors	Participation of private and public sectors
Focus on structures	Focus on networks/strategic coalitions
Formation of a model of various related authorities	Refinement of responsibilities of related authorities
Capacity-building in the Netherlands	Capacity-building both in the Netherlands and other countries
General approach: distribution of capacities for enhanced protection measures	Risk-based approach: balance between protection of interests, threats and acceptable risks in society
Formation of fundamental principles	Presentation of policy (vision)
From ignorance to awareness	From awareness to capability

Table 1 specifically illustrates the changing approach to specific cyber security strategy elements. A change from the formation of initial elements to the refinement of specifics is seen. For example, where the first strategy

formulated fundamental principles of cyber security, the second strategy establishes the presentation of policy (vision). Where the initial strategy formulated the model of related authorities, the second ones focuses on more specific responsibilities. The internationalization method of the cybersecurity phenomena should be noted. The second strategy of 2013 emphasizes capacity building both in the Netherlands and abroad and focuses more on the capabilities with the overall assumption that awareness has already been reached. The second strategy of the Netherlands also highlights a specific action plan laid out in the Annex to the strategy according to each goal.

4. National Cyber Security Strategies of Estonia of 2008 and 2014

The achievements which Estonia made in the area of cyber security came to light in 2007 when Estonia was the first country in the world to be the target of cyber-attacks. Shortly afterwards, in 2008, Estonia adopted its first cyber security strategy. The strategy has a very clear structure – an introduction, cyberspace threats, actions in the cyber security area, enhancement of cyber security in Estonia and implementation of cyber security. According to the Estonian Cyber Security Strategy of 2008, national implementation of cyber security should be based on such principles as cooperation between public and private sectors, protection of critical infrastructure, awareness raising etc. Cyber security threats are defined in the Estonian Cyber Security Strategy of 2008 as potential attacks, which are carried out remotely, using minimal resources and resulting in severe consequences. The action plan emphasizes the protection of Estonian information society and information infrastructure, security of information systems, practical trainings in the area of information security as well as the importance of legal cyber security regulation and international cooperation. To describe legal regulation in the Estonian strategy, a comprehensive review of key documents of international, regional and national legislation as well as of aspects of cooperation of international organizations was conducted.

In 2014, Estonia adopted a new cyber security strategy. It should be mentioned that the Estonian Cyber Security Strategy of 2008 was also considered to be one of the most advanced strategies in Europe (Laasme, 2012). Thus, the new strategy has consistently continued the implementation of most of the goals set in the strategy of 2008. Moreover, the new strategy incorporates new threats and needs, which were not provided for in the previous strategy. It should also be noted that when it comes to content, the new Estonian strategy is more concise. The strategy of 2014 analyses the current situation (the progress achieved in separate sectors, cyber security trends and other challenges). The increasing dependence of Estonia as a country, as well as of its economy and residents on information technology and electronic services is identified as the main challenge. The need for modern legal regulation has been highlighted as additional activity to repel threats listed in the new strategy. When comparing the principles laid down in the Estonian strategy of 2008 and the strategy of 2014, most of the principles identified in the strategy of 2008 can be seen to have prevailed in the strategy of 2014, with the only difference being in the formulation thereof. The main goal provided for in the Estonian Cyber Security Strategy of 2014 for the next four years (2014–2017) is to increase cyber security capabilities and raise the population's awareness of cyber threats, while at the same time ensuring continued confidence in cyber space. The last part of the Estonian strategy of 2014 describes the related authorities responsible for strategic actions and lays down specific deadlines for the implementation of the actions.

In summarising the comparison of both strategies we notice some profound insights. First, a very important aspect of cyber security phenomena – continuity. The new strategy has consistently continued the implementation of most of the goals set in the strategy of 2008. Second, one outcome of this continuity is that many aspects in the second strategy remain the same, only the formulation differs slightly. The second strategy is found to be more concise, itemizing principles of cyber security, the overall objective of the strategy and additional goals.

5. National Strategy to Secure Cyber Space of the United States of 2003 and US International Strategy for Cyber Space of 2011

The first cyber security strategy document of the United States appeared in 2003 when the National Strategy to Secure Cyberspace was adopted. Compared to the strategies of the Netherlands and Estonia examined above, this strategy can be distinguished for its comprehensiveness and scope. In terms of content, the strategy consists of an introduction, threats and vulnerabilities of the cyber space, the national policy and tendentious principles as well as five priorities of the national cyber security.

The National Strategy to Secure Cyberspace of the US of 2003 emphasizes the efforts and priorities of the organization. It also establishes the direction for the actions of government and other organizations. Moreover, this document identifies specific actions to be undertaken by state and local governments, private companies and organizations as well as individuals in order to achieve a higher level of cyber security. Unlike the European cyber security strategies (the Netherlands and Estonia), the US has included each US citizen since 2003, emphasizing that everyone can contribute to the creation and development of cyber security. It is notable, that even if the strategy of 2003 is comprehensive, it distinguishes only three strategic goals. The 2003 National Strategy to Secure Cyberspace presents a vision stating that the protection of cyber security is a complex and constantly evolving challenge. The strategy mentions that this document is the first step to protecting information infrastructures in the long-term. The strategy mentions and distinguishes functions and responsibilities of federal and local governments.

The US International Strategy for Cyberspace was adopted in 2011. Its content consists of four parts: 1. Building cyberspace policy. 2. Cyberspace's future. 3. Policy priorities. 4. Moving forward. Cyber security regulation requires a coherent policy and media attention; it is a complex regulation of state and federal government, including various regulatory methods and areas of application (Thaw, 2014). Thus, the US strategy of 2011 emphasizes a strategic method based on success building, principles and recognizing challenges. This strategy is based on fundamental principles, such as respect for fundamental freedoms, recognition of privacy and free movement of information. The goal of the US International Cyberspace Strategy of 2011is to work at the international level in order to promote open, interconnected, secure and reliable information and communication infrastructure, which supports international trade and commerce, strengthens international security and fosters free expression and innovation. The appropriate response to cybercrime can be achieved solely through international cooperation (Rosenzweig, 2012). In order to achieve this goal, the USA has been constantly building an environment with existing norms of responsible actions, reliable partnership and the support of the country's cyberspace under the rule of law. It should be noted that the development of such cyberspace norms in the country means that the country's actions have become predictable, and misunderstandings leading to conflict situations can be avoided. The idea behind the development of cyberspace norms emphasized in the strategy can also be found in scientific doctrine examining the occurrence of potential proactive cyber security norms in international law (Craig, Shackelford, Hiller, 2015).

Unlike other cyber security strategies, the US strategy of 2011 emphasizes the contribution of the United States themselves into the future of the strategy. The diplomatic goal of the United States is to develop initiatives and a common understanding of the international environment, where the states would work together as related responsible authorities. Moreover, the strategy mentions that the states should strengthen partnership, protection, security of information networks and deterrence against hostile acts.

Summing up it might be concluded that compared to the European strategies, both US strategies emphasize the involvement and contribution of each individual to the cyber security improvement process. Another difference of the US strategies might be noticed in the description of the aims of the strategies. While both strategies are very

comprehensive, both establish three (2003 strategy) and only one (2011 strategy) goal. In addition, the aspect of cyber security as a global matter is stressed in both of the US strategies.

6. National Information Security Strategy of Finland of 2008 and Cyber Security Strategy of Finland of 2013

The National Information Security Strategy adopted in Finland in 2008 is aimed at making each day in the information society secure and reliable for everyone. The vision of the strategy is the confidence of these bodies in the fact that information is secure when using various communication technologies and related services. The priorities of the National Information Security Strategy of Finland of 2008 establish the principles for the protection of a critical information society and international network cooperation. Finland is an integral part of the global information economy, and many threats are of international nature. Therefore, resistance to such threats is based on good preparation and efficient expansion of the international cooperation network and a clear vision of the future in the identification of threat signals.
The Cyber Security Strategy of Finland was adopted in 2013. The content of the strategy consists of four parts and annexes [24]: 1. Introduction. 2. Vision for cyber security. 3. Cyber security management and the national approach. 4. Strategic guidelines for cyber security. The strategy presents the vision, approach and strategic guidelines of cyber security. Unlike other strategies, this one establishes that cyber security is not exclusively a legal category, the adoption whereof would mean the conferral of new competences to institutions and other state establishments. Thus, this strategy is not aimed at creating new responsibilities and powers for the authorities.

The vision of Finland's cyber security is that Finland can secure its vital functions against cyber threats in all situations. Citizens, authorities and businesses can effectively utilize a safe cyber domain and the competence arising from cyber security measures, both nationally and internationally. Finland's strategy of 2013 is linked to the national information security strategy of 2008. It establishes that cyber security depends on efficient organization of information security. In other words, cyber security regulation is viewed holistically. Thus the implementation of cyber security is based on efficient and all-inclusive collection of information and the analysis thereof nationally and internationally. This is the only way in which comprehensive preparedness against cyber-attacks can be achieved. Good management of cyber security allocates responsibilities and functions among state authorities, private entities and the public. Cyber security must meet functional and technical requirements. The strategy mentions investments and trainings in research and development and the fact that Finland will contribute to these initiatives. By way of conclusion it might be stated that similar to the Estonian case, Finland emphasizes the element of continuity in drafting the strategy of 2013.The trend of moving from the level of fundamental provisions to a more strategic approach can be noticed in the comparison of both documents. However, unlike other countries, the new strategy of 2013 establishes that cyber security is not exclusively a legal category, thus this strategy is not aimed at creating new responsibilities and powers for the authorities.

Conclusions

The historical development analysis of cyber security strategies of all the countries above revealed one essential feature – the change of document provisions, which undoubtedly reflects the progress of cyber security in real life. The strategies obviously have to reflect the real life situation (Rosenzweig, 2012). From our analysis of the different cyber security strategies, we have noticed several important trends.

At first, if the initial strategies talked about the formation of fundamental provisions, the second ones had a more specific focus, such as the presentation of policy and vision. The first strategies emphasized structures and the formation of a model of responsible authorities, while the second strategies focus on strategies and refinement of

institutional responsibilities. The first strategies raised awareness of cyber security, while second strategies talk about the development of abilities in the cyber security area. The second strategies are more specific and most of them enclose specific action plans in the cyber security field.

The second, the analysis also revealed the importance of the global approach in cyber security phenomena. The majority of first strategies emphasized the cyber security capacity-building inside the country itself, while almost all the second strategies emphasize the building of capacities internationally. A particularly significant example of the current tendency is revealed in the analysis of the US strategy of 2011. While emphasizing the internationality of cyber security, the diplomatic goal of the US is to create initiatives and a common understanding of the international environment, which would work for the mutual benefit of cyber security. In so doing, the US assumes liability for cyber security of the entire international community.

The third, the consistency approach in building future cyber security strategies can be noted. Many second cyber security strategies emphasized the criterion of continuity. For example, since the Cyber Security Strategy of Estonia of 2008 was an advanced document, the second Cyber Security Strategy of 2014 distinguishes the emphasis on continuously developing confidence in cyber space. The US cyber security strategy of 2011 stresses the predictability of cyber security, which might be linked with the consistency approach.

The fourth, the planned specific deadlines for the implementation of the strategies can be distinguished herein as one of the progress indicators contained in the provisions of many second generation strategies themselves. Planned specific deadlines emphasize specific matters, certain actions and authorities responsible. Planned deadlines refer to the achievement of the results.

Acknowledgements

This article is part of the research 'Analysis and adaptation of EU and NATO cyber security strategies: Lithuanian cyber security model', funded by the Research Council of Lithuania (Grant No. MIP-099/2015/PRC-36).

References

Allabouche, K.; Diouri, O.; Gaga, A.; El Amrani El Idrissi, N. 2016. *Mobile phones' social impacts on sustainable human development: case studies, Morocco and Italy*. Entrepreneurship and Sustainability Issues Vol. 4. No. 1, pp. 64-73. DOI: http://dx.doi.org/10.9770/jesi.2016.4.1(6)

Bambauer D. E., 'Schrodinger's Cybersecurity'. University of California: *Davis Law review*. Vol. 48. No. 3. 2015. p. 798.

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 Vol. 5 No.3, pp. 411-422. DOI: http://dx.doi.org/10.9770/jssi.2016.5.3(9)

Cezar P., Cyber security – current topic of national security. *Public security studies*. Vol. II. No. 4(8). Dec 2013. p. 25

Craig A.N., Shackelford S.J, Hiller J. S., 'Proactive cybersecurity: a comparative industry and regulatory analysis'. *American business journal*. March 2015. [interactive] [2015] [viewed on 23-11- 2015] SSRN: http://ssrn.com/abstract=2573787

Cyber security strategies of all countries of the world and years of adoption thereof are available on the website of ENISA. [interactive] [2015] [viewed on 2015-11-09]. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

Cyber Security Strategy of the European Union [interactive] [2015] [viewed on 26-10-2015]. https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

Cyber Security Strategy of the Netherlands of 2014. p.8. [interactive] [2015] [viewed on 18-11-2015]. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf

Directive of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union. [interactive] [2016] [viewed on 19-09-2016]

Estonian Cyber Security Strategy of 2014. p.7. [interactive] [2015] [viewed on 23-11-2015]. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies ncsss/Estonia_Cyber_security_Strategy.pdf

Estonian Cybersecurity Strategy of 2008. p. 7. [interactive] [2015] [viewed on 18-11-2015. http://www.eata.ee/wp-content/uploads/2009/11/Estonian_Cyber_Security_Strategy.pdf

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Klimburg A. *National Cybersecurity Framework Manual*. NATO CCDCOE, 2012. https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

Laasme H.. The role of Estonia in developing NATO'S cyber strategy. Cicero foundation great debate paper. No.12/18. 2012. P. 9. [interactive] [2015] [viewed on 23-11- 2015]
SSRN:http://www.cicerofoundation.org/lectures/Laasme_%20Estonia_NATO_Cyber_%20Strategy.pdf

National Cyber Security Strategy of Finland of 2013. [interactive] [2015] [viewed on 29-12-2015]. https://ccdcoe.org/cyber-security-strategy-documents.html.

National Cyber security Strategy of the Netherlands of 2011. p.3. [interactive] [2015] [viewed on 18-11-2015]. https://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011

National Strategy to Secure Cyber Space of the United States of 2003 [interactive] [2015] [viewed on 29-12-2015]. https://ccdcoe.org/cyber-security-strategy-documents.html .

Rosenzweig P., 'Making Good Cybersecurity Law and Policy: How Can We Get Tasty Sausage?' *A journal of law and policy for the information society*. Vol. 8(2). 2012. p. 398.

Sales N.A., 'Regulating Cybersecurity'. *North-western University Law Review*. Vol. 107. No. 4. p. 1567.

Samašonok, K.; Išoraitė, M.; Leškienė-Hussey, B. 2016. *The internet entrepreneurship: opportunities and problems*, Entrepreneurship and Sustainability Issues Vol. 3 No. 4, pp. 329-349. DOI: http://dx.doi.org/10.9770/jesi.2016.3.4(3)

Shoemaker, D.; Conklin, A., *Cyber security: the Essential body of knowledge*. Course technology. 2012. p. 11.

Thaw D. The efficacy of cybersecurity regulation. *Georgia state university law review*. Vol. 30(2). 2014. p. 291

The United States Computer Science and Telecommunications Board research, accessed online. [interactive] [2015] [viewed on 05-11-2015] http://sites.nationalacademies.org/CSTB/index.htm

Ventre D., *Chinese Cybersecurity and Defense*. London, John Wiley & Sons, Inc, 2014.

Darius Štitilis is professor at the Mykolas Romeris University. 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.
ORCID ID: orcid.org/0000-0002-9598-0712.

Paulius Pakutinskas is associated professor at the Mykolas Romeris University. 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.

Inga Malinauskaitė is a lecturer and PhD student at the Mykolas Romeris University. 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.
ORCID ID: orcid.org/0000-0001-5693-7300