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
2016 December Volume 6 Number 2
http://dx.doi.org/10.9770/jssi.2016.6.2(1)

CONCEPTS AND PRINCIPLES OF CYBER SECURITY STRATEGIES

Darius Štitilis[1], Paulius Pakutinskas[2], Uldis Kinis[3], Inga Malinauskaitė[4]

[1,2,4]Mykolas Romeris University, Ateities st. 20, LT-08303 Vilnius, Lithuania
[3]Rigas Stradins university, Latvia

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

Received 17 March 2016; accepted 26

Abstract. In the last few decades, the understanding of security has been changing. New areas emerged which may influence security facets, which were not urgent earlier. Now those facets can endanger individual persons or even states. Breaches of cyber security, separate attacks or intense cyber wars are becoming more usual than conventional wars in the physical space; violations of cyber security may cause great damage, ruin businesses or even temporarily paralyze full-fledged functioning of individual states or regions. Many countries of the world, realizing that such a threat is real, adopted Cyber Security Strategies; for some countries, this is not the first version of such a strategy. This article examines the place of Cyber Security Strategies in the system of state documents, the nature and importance of such strategies as well as whether they are binding on individuals and institutions. The article explores in more detail the principles of ensuring cyber security provided for in such strategies, i.e. the principles identified by the states, as important for ensuring cyber security. It is discussed why these principles are so different in the strategies of individual states.

Keywords: concepts, principles, cyber security, European Union (EU), North Atlantic Treaty Organization (NATO).

Reference to this paper should be made as follows: Štitilis, D.; Pakutinskas, P.; Kinis, U.; Malinauskaitė, I. 2016**.** Concepts and principles of cyber security strategies, *Journal of Security and Sustainability Issues* 6(2): 197–210. http://dx.doi.org/10.9770/jssi.2016.6.2(1)

JEL Classifications: F5, F52, K42, K24

1. Introduction

Increasing possibilities of hardware and software, growing Internet speed and importance of wired and wireless data transfer, the emergence of big data and cloud computing services, take-over by smart phones of increasingly more human communication functions, and emerging of other functions important to people means that information technologies play an increasingly more important role in our lives (Fuschi, Tvaronavičienė 2014; Laužikas et al. 2015; Ignatavičius et al. 2015; Grubicka, Matuska 2015; Rezk et al. 2015; Tvaronavičienė et al. 2016; Allabouche et al. 2016; Pauceanu 2016; Rezk et al. 2016; Samašonok et al. 2016; Prause 2016; Korauš et al. 2016). Information technologies are common not only in personal relationships, business, but also in state governance, military systems (which, historically, had a strong impact on the development of this area), science, etc. There are few areas where information technologies do not have an important or decisive impact. Such penetration of information technologies influences many areas of life, and this influence is so major that disturbances to information systems may paralyze one or another function of the state. For this reason, possible occupation or disturbance of information systems, or another impact thereon, are of interest not only to individual offenders or organized mafia groups, but also to official states and their governments, however, often they do not make such activities public or even deny and hide them. Dependence of human activities on information technologies will only increase in the future. Technological achievements are developing in a very

dynamic manner, this also influences possibilities to have an adverse impact, using such technologies, on many areas of human activities, both those mentioned above and those not mentioned, therefore, the issues related to cyber security become increasingly more important. It is easiest for the states to fight adverse phenomena on their territories and jurisdictions, while cyberspace virtually defies state borders, therefore, development of cyber security on an inter-regional and international level becomes an important factor. This study will examine why the present strategies are still so different and whether a possibility exists to single out common principles so that all states find it easier to seek cyber security objectives.

In order to assess the formal preparedness of states to address cyber security questions, it is necessary to analyze regulatory acts and other documents issued by them. In many states, an important constituent part of documents is Cyber Security Strategies. To be able to evaluate the place of these documents in the system of documents of states as well as the importance thereof, it is necessary to answer several particularly important questions, which will be analyzed in this article. It is also crucial asses the means, used for regulation of social relations in the area of cyber security and the typical principles (of a certain field of social sciences) which are used or new principles, which are created exclusively for addressing cyber security issues.

Novelty and originality. In the drawing-up of cyber security strategies and other regulatory acts, it is vital to elaborate on the principles for the creation and development of a cyber security strategy as well as the development and further implementation (application) of legal norms. So far, a more thorough piece of research of cyber strategies has not yet conducted. It is reflected by practice, because the majority of strategies identify different principles and a different content thereof.

A practical and scientific significance. Having identified the place of a strategy - as a document, in the system of documents, as well as the purpose thereof and having systematized and elaborated on the principles of cyber security strategies, it will be easier to develop and improve cyber security strategies and other regulatory acts.

The purpose. To single out and systematize the principles of cyber security strategies.

Methods: Analysis of cyber security strategies and other regulatory acts as well as of scientific literature, comparative analysis, the systematic method.

2. Emergence of Cyber Security Strategies

The first cyber security strategies started to emerge as from the year 2000, however, only 2011 saw a real boom of Cyber Security Strategies and the majority of member states of the European Union and part of the states of the world approved their strategies[1]. That was a period of a break-through when states not only started to consider cyber security issues, but also finally identified them in documents as one of the most important security threats of one's country. Alas, it has to be noted that in democratic states, at least a few years of democratic discussions and coordination of the document elapse, until the approval of a specific document (in this case, a Cyber Security Strategy), i.e. at least one to two years pass as from the realization of cyber security threats, as a fundamental security threat, until the approval of the strategy. During this period, many areas of state activity became dependent on computers, the Internet and other elements of the electronic space. These data is reflected in various types of statistics, for instance, on e-government prevalence, e-banking development, etc. One of the simple and illustrative pieces of data illustrating the turning-point in the importance of cyber security is the number of households with Internet access and the number of individuals using the Internet. We can compare the correlation between the dates of emergence of the strategies and the prevalence of the Internet, which is presented in the charts provided below (Fig. 1, Fig. 2).

[1] More information is available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

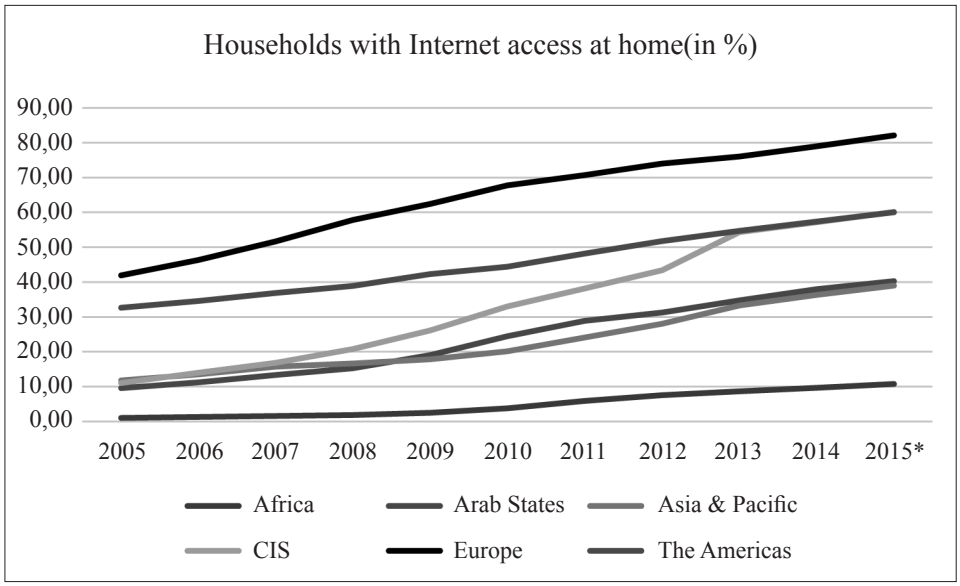

Fig.1. Internet access at home

Source: ITU World Telecommunication/ICT Indicators database.

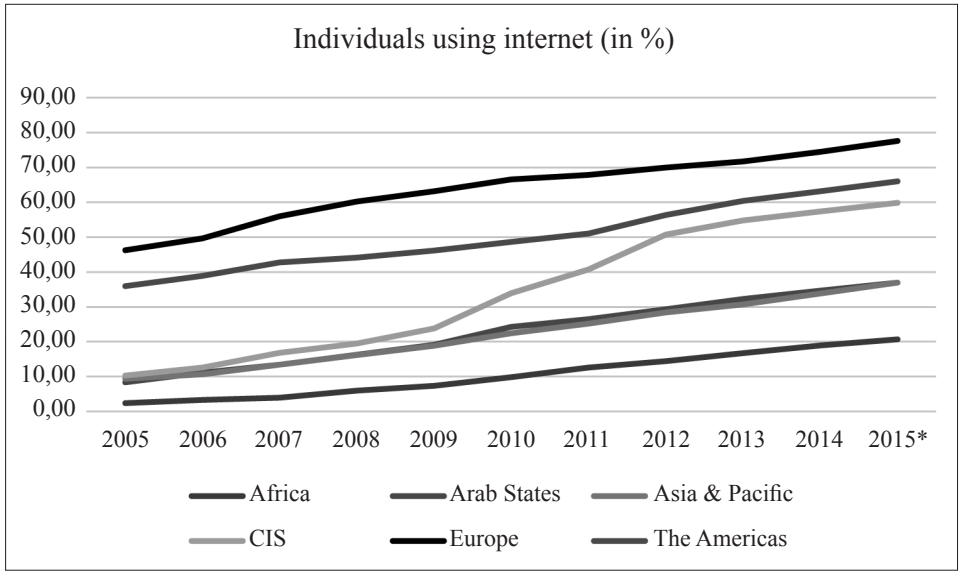

Fig.2. Internet users

Source: ITU World Telecommunication/ICT Indicators database.

It is noteworthy that since the time when, in the leading markets (Europe and America), about 40 per cent and more of users and households started using the Internet, the issue of cyber security has become critical.

It is also important to take into account the prevalence of breaches of cyber security. Every year, target groups and organizations of cyber attacks are different, however, the presented charts show what a wide circle of interests is violated by cyber attacks. It should be noted that the interests of a state are violated not only by those attacks which are aimed directly at the government, but also by the ones which are also able to have an adverse effect on other critical infrastructures and organizations or otherwise disturb the activities of a state or members of society (Fig. 3).

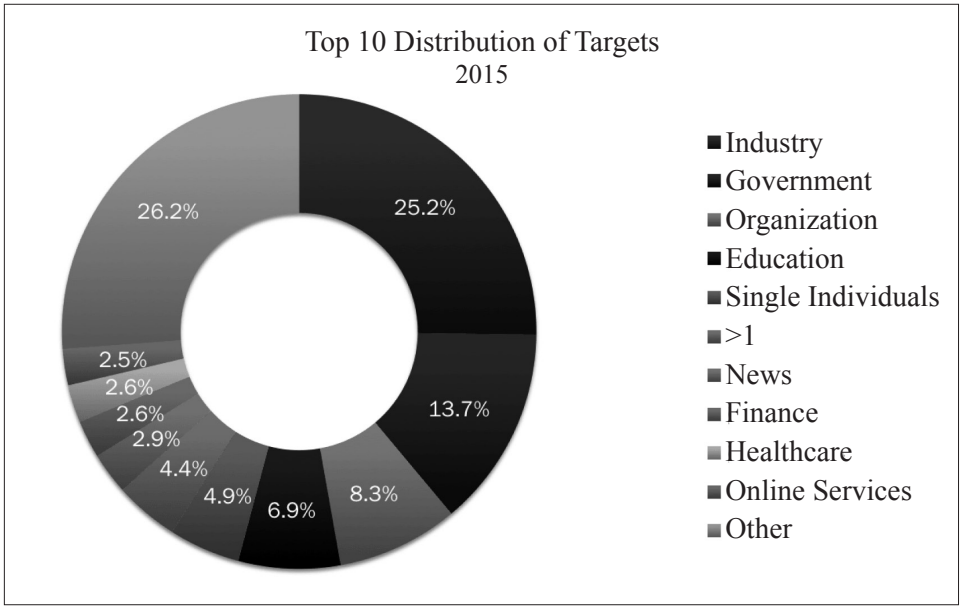

Fig.3. Targets, Organizations and attack statistic

Source: http://www.hackmageddon.com/2016/01/11/2015-cyber-attacks-statistics/

3. Why are Strategies Important?

Once we have identified that cyberspace is, or rather violations of relations created in this space are, a security threat, we face questions, which has to be addressed, and these questions differ from the questions and solutions thereto known to us historically. We will not find cyber security answers either in classical management, or in the military science or law, even though such problems as security, wars, crimes or legal regulation are not new and have a long history. What, then, makes this entire question so specific? Convergence of all these questions, following a change in technological possibilities, makes cyberspace and threats arising therefrom a qualitatively new question requiring a new approach and solutions.

The compilation of all questions, mentioned above in this chapter, and the knowledge possessed into one place does not give a uniform result; it is also confirmed by the variety of effective strategies, even though there are initiatives to make them more uniform (e.g. the EU's and other initiatives), however, so far even cyber security strategies of neighbouring countries or countries with a similar pattern of development have been particularly different. Overall, the objective of all cyber security strategies is similar, because of the intention to fight insecurity challenges in cyberspace and regulate them, however, the description of achieving these objectives and the realization thereof as well as the very strategy documents are very different.

4. Security, Definitions and Changes in the Understanding of the Problem

When talking about cyber security we are addressing fundamental security questions, which were understood in a completely different manner at the beginning and in the middle of the previous century. Especially after the Second World War, security has found major attention in the fields of International Relations and its subdiscipline, security studies. Security studies evolved during the nuclear age and were originally foremost about the study of the threat, use and control of military force, as one proponent of security studies, Stephen Walt, stated. They were mainly concerned with the military strategy and giving policy advice to the military[2]. Since the cold war, the study of security has come a long way. Most importantly, as Emma Rothschild has reminded us, during the past two decades or so, the concept was first extended downwards from states to individuals, upwards from the nation to the biosphere and horizontally from the military to the economic, social, political

[2] BARBARA LÜTHI (2011). Perspectives on Security in Twentieth-Century Europe and the World. Contemporary European History, 20, pp. 207-214. doi:10.1017/S0960777311000063.

and environmental[3]. While examining cyber security questions, we face a lack of definitions or non-uniform interpretation thereof, which could also be noticed at the level of presentation and disclosure of principles. It is crucial that even a threat is defined differently, therefore, different means for the reduction of the threat are employed.

5. Nature of a Strategy Document

While exploring the origin of the word "strategy", one may notice a close link thereof with the military science. Encyclopaedias indicate the origin of this concept and the connections thereof with appropriate areas of activity. The word "strategy", derived from Greek, originally meant the "art of the general", or "generalship". It has long since been broadened to include also the art of the admiral and of the air commander. So dynamic and pregnant a word is bound to be applied also to numerous other kinds of competitive situations, including commerce and games, and today one speaks of testing various "strategies of play" over a broad range of game situations[4]. A strategy: To ancient Greeks, *strategos*, from which we derive "strategy", meant simply the general's art; a modern definition, however, would generalize the meaning to a reasoned relationship among military means and the ways they might be used to reach the ends of national policy[5]. Both definitions, which have been provided, specify the military origin of the word but note that this word is also applied in many other areas of activity. There also exist very simple definitions of a "strategy", for instance, (i) a planned series of actions for achieving something; (ii) skilful planning in general[6]. The word "strategy" is very closely linked with another word originating from the military science, "tactics". "Tactics" are a means by which a strategy is carried out[7]. This means that a strategy should be achieved using "tactics"; in the case in question, separate actions and maybe even laws could be called tactical means.

According to their territorial nature, strategies may be:
- National,
- Regional,
- International and
- Global.

Currently, dominating cyber security strategies are national; the majority of the states examined have their own strategies, and for some countries, their strategy is not the first one, however, there are several regional strategies (for example, European Union) or strategies based on a certain affiliation to concrete organizations (for instance, NATO). At this point in time, there are no international or global strategies, but there exist significant initiatives, for example, The ITU National Cybersecurity Strategy Guide. If a uniform global cyber security strategy were adopted and then accepted by the majority of countries of the world, this would enable the unification of national strategies. That would be a particularly important factor influencing the solution of cyber security questions, however, there is no doubt that it will be hard to achieve that because some states arrange cyber attacks themselves for various purposes and uniform agreement will be difficult.

In order to examine the principles, it is necessary to assess which branch of social sciences these principles will belong to and what is the meaning thereof. It is important to answer the question as to what strategies are and what the purpose thereof is. This question has been analyzed quite little in the theory of social sciences. If we assessed that as "legal strategy", this concept has other meanings which are applied in choosing legal actions in order to achieve appropriate legal objectives (for instance, to win a case); in the case in question, this concept and interpretations are completely inappropriate.

---

[3] Rothschild, Emma. What is Security? Daedalus 124, 3 (1995), 53–98.

[4] "Strategy." International Encyclopaedia of the Social Sciences. 1968. *Encyclopedia.com.* 17 Jan. 2016. Available on the Internet: <http://www.encyclopedia.com>.

[5] John Whiteclay Chambers II. "Strategy." The Oxford Companion to American Military History. 2000. *Encyclopedia.com.* 17 Jan. 2016. Available on the Internet: <http://www.encyclopedia.com>.

[6] Longman Dictionary of Contemporary English. Available on the Internet: <http://www.ldoceonline.com/dictionary/strategy>

[7] Read more at: http://www.businessdictionary.com/definition/tactics.html#ixzz3xV8d6m3C

It is vital to answer the question as to what kind of act a strategy is. Unfortunately, there are no unambiguous answers to this question, and probably there cannot be just one answer, because different states have their own specific features, i.e., for example, acts called strategies are passed departing from the means of legislating typical of legal norms or, conversely, they are passed in accordance with the procedure typical of adoption of legal acts by appropriate authorized institutions and comply with the majority of requirements for legal acts and legal norms, i.e. the formal definition and systematic character.

As mentioned above, it is important to assess what a strategy is in such a case. There is more than one definition, however, one of the short and simple definitions is the following: "A strategy is a plan for action intended to accomplish some goal"[8]. This definition m be applied in individual situations and in order to achieve more abstract objectives, therefore, the meaning of a legal strategy mentioned above may be the selection of concrete legal means in order to achieve an objective. From the systematic point of view, Cyber Security Strategies may be regarded as an action plan to achieve certain cyber security objectives; therefore, such strategies should focus on appropriate formulation of objectives and determination of how these objectives are to be achieved. In the definition of objectives and means to achieve them it is also important to formulate appropriately principles, which shoul be observed in order to achieve the objectives.

Contemporary process of legislation and democracy enables a fragmented adoption of legal norms by amending separate legal norms or parts thereof as well as adaptation of the norms to the changing social relations taking into account only separate incidents and in a very short-term perspective. Such process of legislation does not comply with the fundamental principles, i.e. predictability of law, legitimate expectations, stability of the state, etc. In order to avoid such bad practice of legislation, appropriate methodologies and means are necessary in order to improve the legislative process. How and where should the conceptual objectives and principles of the legislative process be provided?

The concept of a strategy, which originated from the military science, has been widely used in business, however, a strategy is also necessary while planning the adoption of legal norms and the activities of a state in one or another area.

Problems arise not only during the stage of development and realization of legal regulatory acts, but also during the earlier stages, i.e. while determining objectives and principles of regulatory acts to be adopted as well as the timeframe for coming into effect thereof, the funding of legal means established by legal norms, etc. The norms will be efficient only if they are in conformity with the social situation, clear objectives of legal norms are identified and there is a plan as to how the objectives will be achieved. The establishment of objectives and principles for adjustment of social relations makes it possible to forecast possible changes in norms more clearly and at the same time avoid very frequent and erroneous changes in them.

This early stage, when objectives as well as means and measures to achieve the objectives are determined, is called a strategy.

A legal strategy includes prospective planning and forecasting as well as a conceptual and long-term foresight of problems in the development of law-making.

Some strategies comply with the majority of requirements for legal norms and may be considered as legal norms with organizational elements though; however, strategies of some states may not be regarded as legal norms because they are not in conformity with all the formal attributes of a legal norm. These attributes are the following: normative nature, formal definition, universal mandatory character, guarantees of universal mandatory character (mutual benefit and a state's coercion) and systematic character. Separate strategies have a declarative, organizational nature, i.e. they do not prescribe a rule for concrete behaviour, are not universally mandatory, etc.

[8] Martha C. Nussbaum, Flawed Foundations: The Philosophical Critique of (a Particular Type of) Economics, 64 U. CHI. L. REV. 1197, 1199 (1997). 7 (defining "strategy").

Considering the circumstances mentioned above, it is possible to maintain that a strategy is an organizational document which provides for measures and means to be chosen in order to achieve the objectives established in the strategy.

Taking into consideration that strategy is a high-level document it is important to find what level issues need to be developed in this document. The variety of issues discussed in existing national cybersecurity strategies are quitting big, including depth how these issues are discussed. The problem is to see all the system of state documents, therefore it is good to fix just very high level issues (like vision, goals, principles, etc.) in the strategy and to do not go more in details. Why it is important? We can divide strategies into short, medium and long-term strategies. It could be good and important discussion what particular time periods are short, medium and long for strategies in cyber security (so rapidly changing field of activities), but we need to have understanding of all of these three periods to do not lose concentration into main aims, but to stay flexible enough at the same time. Therefore, it is very important not to go into details in strategy, and to divide clearly what we can solve in the strategy, and what - in the laws.

6. Singling out Principles in Separate Strategies

The word "principle" derives from the Latin word *principium*. This word also has a number of meanings: (1) a fundamental truth or proposition that serves as the foundation for a system of belief or behaviour or for a chain of reasoning; (2) a fundamental source or basis of something[9], etc.

According to dictionaries of international words, "principle" may be described as "a conviction determining the norms of a human being's relations with the reality as well as his/her behaviour and activity". Based on the provided description, "principle" is understood in the most general sense, as a steering source substantiating the content, concrete manifestations or individual elements of a certain phenomenon. Such is, probably universally recognized, the meaning of this concept[10].

The cyber security problem encompasses many areas of human activity, and originates from a technological change, i.e. technologies enabled the emergence of the security problems under discussion. However, that is not technologies that cause problems, but people using technological possibilities, and adapting them for their purposes, i.e. the majority of problems is not of technological nature but has to do with the relation of a human being with technologies and relations of people with other people (for instance, systems are disturbed, in a targeted manner, not by technologies themselves (accidental disturbances, though, also happen due to imperfect technologies), but by people seeking selfish purposes (money, power, influence, etc.), i.e. many questions are social and they are examined by social sciences, therefore, to resolve them, the principles of social sciences are to be applied, such as the principles of law, management, economics and others.

In the examination of the principles of strategies, the main source is the texts of these strategies. Some strategies do not single out clear principles or indirectly mention isolated principles (strategies of Albania, the Netherlands, Luxembourg, Lithuania, Italy, Hungary and France), other countries single out only several clear principles in their strategies (United Kingdom (three), United States of America (three), Latvia (four), Ireland (three) and Czech Republic (three)). Some countries single out very many principles (Germany (seven), Finland (eight), Romania (eight), Estonia (eight) and Turkey (as many as thirteen)).

Some strategies clearly single out concrete principles and classify them (The strategy of Austria: "Principles related to the very strategy: comprehensiveness, integrity, proactivity and solidarity. II. Universal ICT security

[9] "principle." The Oxford Pocket Dictionary of Current English. 2009. *Encyclopedia.com.* 17 Jan. 2016. Available on the Internet: <http://www.encyclopedia.com>.

[10] "principle." The Oxford Pocket Dictionary of Current English. 2009. *Encyclopedia.com.* 17 Jan. 2016. Available on the Internet: <http://www.encyclopedia.com>.

principles: confidentiality, integrity, mandatory application, authenticity, accessibility and protection of personal data. III. Fundamental principles: rule of law, subsidiarity, self-regulation and proportionality."), in the strategies of other countries, chaos is felt and one can discuss whether what is called principles indeed are principles.

The Cyber Security Strategy of the European Union singles out five principles:
1) What applies in the physical space, also applies in the electronic space;
2) Protection of fundamental rights;
3) Access for all;
4) Management of various players;
5) Common responsibility.

When discussing these principles, it is vital to single out the most specific and important principles as well as doubtful principles. Starting with the doubtful principles, one should single out universally effective principles of general nature and principles provided for in other important documents, for example, "Protection of fundamental rights". Does singling out of this principle, as a specific or general cyber security principle, bring something new? Would, in the absence of the Cyber Security Strategy of the European Union, this principle be ineffective or effective to a smaller extent? The content of this principle is clear enough, well-detailed in appropriate international regulatory acts and checked over and over again by authoritative international courts; and the presentation thereof in this strategy is not necessary, even though possible by showing that this is a guideline which is very important when addressing violations of this type of security, i.e. that fundamental human rights may not be sacrificed because of security solutions. Another doubtful cyber security principle is "Access for all". This principle hardly increases security, rather reduces it, however, this principle is important from another point of view, i.e. in order to create a free and democratic community of virtual space but quite often this is what determines the vulnerability of such virtual space.

There is no doubt that the principle "What applies in the physical space, also applies in the electronic space" is a specific principle. This principle or principles very close to it are also indicated, in one way or another, in other regulatory acts regulating electronic space, for instance, the principle of non-discrimination of electronic form, etc. Another principle, which is specific indeed, as to how cyber security may be achieved is the principle of "Management of various players", because cyber security may also be achieved using other principles, for example, the principles of centralization of appropriate resources, control or restriction, however, the concrete strategy says that cyber threats may be managed through various players.

As already mentioned, some principles could be left unmentioned, however, the presentation of all important principles in one place is valuable at least because all principles are to be applied only as part of a system, and singling out of the principles and including them into one document enable a more clear assessment of the entirety and system of principles.

NATO singles out three principles:
(1) Prevention;
(2) Resilience;
(3) Non-duplication.

This list of principles is much shorter than the lists of principles of various countries, however, these principles may be singled out as specific cyber security principles.

For a deeper analysis, a comparison may be made between the principles used by several different states.

In the 2014 strategy of Estonia, eight principles of ensuring cyber security are provided for:
1. Cyber security is an integral part of national security; it supports the functioning of the state and society, the competitiveness of the economy and innovation.
2. Cyber security is guaranteed by respecting fundamental rights and freedoms as well as by protecting indi-

vidual liberties, personal information and identity.
3. Cyber security is ensured on the basis of the principle of proportionality while taking into account existing and potential risks and resources.
4. Cyber security is ensured in a coordinated manner through cooperation between the public-, private- and third sectors, taking into account the interconnectedness and interdependence of the existing infrastructure and services in cyberspace.
5. Cyber security starts with individual responsibility for safe use of ICT tools.
6. A top priority in ensuring cyber security is anticipating as well as preventing potential threats and responding effectively to threats that materialize.
7. Cyber security is supported by intensive and internationally competitive research and development.
8. Cyber security is ensured via international cooperation with allies and partners. Through cooperation, Estonia promotes global cyber security and enhances its own competence.

In this strategy, in addition to more general principles, which are frequent, there are also principles which are indeed interesting and important in the fight against cyber violations, for instance, how to use intensive and internationally competitive research and development for a new and rapidly-changing medium. This is a very important principle of ensuring cyber security, which is undoubtedly specific.

Some principles are also found in other strategies, for example, the principles of respect for fundamental rights, proportionality, cooperation of public and private sectors, personal responsibility and international cooperation.

In the 2014 strategy of another Baltic State, Latvia, the state principles have been formulated in a brief manner but clearly disclosed and linked to the objective: "The aim of the cyber security policy is a secure and reliable cyberspace, which ensures a safe, reliable and continuous supply of services essential for the state and society. In implementing the cyber security policy, the following principles are being used – development, cooperation, responsibility and openness." These four principles have been disclosed very thoroughly:
Development – it is possible to protect against rapidly growing threats in cyberspace only by constantly and systematically developing and improving skills in the ICT sector and its security specialisation.

Cooperation – the effective protection against threats in cyberspace unrestricted by geographical boundaries of countries or administrative boundaries of institutions is only possible through cooperation at both the national and international level.

Responsibility – it is possible to effectively reduce risks in cyberspace only if all parties involved in cyberspace, including individuals, state institutions and private businesses, are informed about and aware of the effects of their activity or inactivity on their own security and the security of others.

Openness – the cyber security policy is to be implemented by facilitating the accessibility of information and communication technology while respecting the rights and fundamental freedoms of an individual, searching for a balance between freedom, privacy and security as well as promoting good practices, ethics and standards in cyberspace.

Austria (in its 2013 strategy) singles out two important groups of principles:
"The universal Principles of ICT Security for a Digital Austria are fully applicable to cyber security: confidentiality, integrity, mandatory application, authenticity, availability as well as privacy and data protection."

The more important principles are singled out separately in the Austrian strategy and their content is explained:
"The following fundamental principles are in any case applicable to the area of cyber security:
The rule of law: Governance in the area of cyber security has to meet the high standards of the rule of law of the Austrian administration and guarantee compliance with human rights, in particular privacy and data protection, as well as the freedom of expression and the right to information.

Subsidiarity: Cyber security is a legal asset. Therefore, the state pledges its strong commitment to the protection of this legal asset. However, it cannot and should not assume sole responsibility for protecting cyberspace. The owners and operators of information and communication technology (ICT) are primarily responsible for protecting their systems. The following principle shall apply: "Self-commitment if possible, regulation if necessary".

Self-regulation: Efforts should in general be made to increase the level of protection through the actors' own initiatives on the basis of code of conducts, standardisation and certification.

However, it remains the task of the state to create the regulatory framework for protecting the ICT of enterprises and private persons and to support self-regulation in the private sphere.

Proportionality: Measures to increase the level of protection and the respective costs have to be proportionate to the respective risk and to the possibilities of limiting these threats."

While analyzing the principles singled out in other strategies, one may notice that these principles are particularly different, however, the strategies mention the general principles of law and the special cyber security principles (both legal principles and other principles of social regulation). It is crucial to notice that the general principles of law are included incoherently, by singling out some of them, but not mentioning others; due to this, there remains no systematic understanding of the general principles of law, which is a faulty practice. To sum up, the enumeration of the general principles of law is possible and important, but they should be disclosed in a systematic and consistent manner; if that is not done, the enumeration thereof is not necessary and is not recommendable. It makes no sense to repeat, in the strategies, the general principles of law which are provided in Article 38 (1) (c) of the Statute of the International Court of Justice as "general principles of law recognized by civilized nations", because these principles must be effective in civilized countries as it is, therefore, it is advisable to focus on the specific principles which are characteristic only of strategies or are used in order to ensure cyber security.

The situation is completely different when it comes to the special principles. If we maintain that a strategy is a consistent universal act establishing a cyber security regulation strategy, then the identification of the special principles, and maybe even the disclosure of the content thereof, is vital. Applying the principles provided for in the strategies, it is possible to develop legal regulation more consistently as well as develop other social relations.

7. Conclusions

The principles of a democratic society make it possible to create regulation in a fragmented manner according to separate initiatives raised lawfully by interest groups, however, for the entire regulation process to be consistent, planning and the establishment of guidelines in regulation are necessary; the process of planning and forecasting is established by a strategy. A strategy may be a regulatory act possessing all the attributes of a regulatory act, however, even if a strategy does not possess certain attributes of a regulatory act, it most often is an organizational document which describes and identifies a problem to be solved as well as establishes objectives and measures and means to achieve the objectives provided for in the strategy. Such a document enables consistent planning, anticipating and forecasting of long-term trends of the development of an appropriate question, which makes it possible to provide for, in a consistent and timely manner, correctional measures of a social relation, including mandatory rules establishing legal norms, which establish and correct society's social behaviour. Strategies have an even greater meaning and value when relatively new phenomena are regulated and when there are no well-established global standards as to how emerging problems should be addressed; this makes it possible not only to appropriately regulate the relations, but also save resources. Forecasting of social relations enables the reduction in the adoption of unnecessary and untimely legal norms, which do not meet the needs, or the establishment of another regulation as well as provides the guidelines as to when it is necessary to adopt appropriate legal norms and different regulation so that one is not late with appropriate regulation of the

relations; this ensures more efficient development of comprehensive regulation.

Cyber security strategies of different states have similar structural elements of a document, for instance, objectives to be achieved which are established, principles, etc. However, the disclosure and description of these elements are quite different. The article has focused on the principles of implementation of cyber security strategies. Strategies identify different principles of social sciences (management, law, politics, economics, military science, etc.). The principles singled out in some strategies raise doubts as to whether they are indeed principles, or maybe they are only means or methods to achieve an objective. Not all strategies identify concrete principles, however, certain strategies single out even more than ten principles. This demonstrates not only the variety of different means to achieve cyber security, but also a different understanding of states as to what should be reflected in the strategies and how. It should be noted that even the EU directives promoting unification do not provide for a need to establish the Principles of Ensuring Cyber Security in national cyber security strategies. While establishing the principles in strategies, it is not necessary to repeat universally acceptable principles of separate areas, for example, law (the supremacy of human rights, etc.), because a strategy may not and does not have a purpose to abolish or amend them; they are effective under other national or international regulatory acts. It is advisable to establish only special principles of cyber security strategies or principles which acquire more importance in the cyber security context than in other areas of human activity. However, it is crucial that the general or special principles included into a strategy would indeed be key for the achievement of cyber security; then, following the identification of such principles in one document, we have a consistent system of principles because principles are applied correctly only in a uniform system, while making one or another principle absolute or attaching too much significance to it may cause damage to the entire system and distort it.

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).

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* 4(1): 64-73. http://dx.doi.org/10.9770/jesi.2016.4.1(6)

Albanian Cyber Security Strategy, 2014. Available on the Internet: <http://www.mod.gov.al/images/PDF/Strategjia_per_Mbrojtjen_Kibernetike.pdf>

Austrian Cyber Security Strategy, 2013. Available on the Internet: <https://www.bka.gv.at/DocView.axd?CobId=50999>
BSA. 2015 EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace. Available on the Internet: <http://cybersecurity.bsa.org/index.html>

Carayannis E.G., Campbel D.F.J., Efthymiopoulos M.P. 2014. Cyber-Development, Cyber_Democracy and Cyber-Defence: Challenges, Opportunities and Implications for Theory, Policy and Practice. New York: Springer.

CCDCOE. 2014 Summit Updates Cyber Defence Policy. Insider news, 24 October. Available on the Internet: <http://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html>

Council of Europe. 2001 Convention on Cybercrime, Budapest, No. 185, 23 November. Available on the Internet: <http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>

Council of Europe. Chart of signatures and ratifications of Treaty 185. Available on the Internet: <http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=P60tWvz9>

Cyber Security Strategy for Germany, 2011. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Germancybersecuritystrategy20111.pdf>

Cyber Security Strategy in Romania, 2011. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/StrategiaDeSecuritateCiberneticaARomaniei.pdf>

Cyber Security Strategy of Belgium, 2012. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/copy_of_BE_NCSS.pdf>

Cyber Security Strategy of the Czech Republic, 2015. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CzechRepublic_Cyber_Security_Strategy.pdf>

Cyber Security Strategy of the United Kingdom, 2011. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/UK_NCSS.pdf>

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Available on the Internet: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF>

Estonian Cyber Security Strategy, 2014. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf>

European Commission. 2001. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, Network and Information Security: Proposal for a European Policy Approach, COM (2001) 298 final, 6 June. Available on the Internet: <https://ccdcoe.org/sites/default/files/documents/EU-010606-NISProposal.pdf>

European Commission. 2006 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, A strategy for a Secure Information Society - Dialogue, partnership and empowerment, COM(2006) 251 final, 31 May. Available on the Internet: <http://ec.europa.eu/information_society/doc/com2006251.pdf>

European Commission. 2013 Commission Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union. February 7. Available on the Internet: <http://ec.europa.eu/digital-agenda/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and>

European Commission. 2013 EU Cybersecurity plan to protect open internet and online freedom and opportunity. Press Release, 7 February. Available on the Internet: <http://europa.eu/rapid/press-release_IP-13-94_en.htm>

European Commission. 2013 Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN (2013) 1 final. Brussels, February 7. Available on the Internet: <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667>

European Commission. 2013 Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. COM(2013) 48 final. Brussels, February 7. Available on the Internet: <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666>

European Commission. 2015 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. The European Agenda on Security. COM(2015) 185 final, Strasbourg, 28 April. Available on the Internet: <http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf>

Finland‘s Cyber Security Strategy, 2013. Available on the Internet: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/FinlandsCyberSecurityStrategy.pdf

Fuschi, D.; Tvaronavičienė, M. 2014. Sustainable development, Big Data and supervisory control: service quality in banking sector, *Journal of Security and Sustainability Issues* 3(3): 5-14. http://dx.doi.org/10.9770/jssi.2014.3.3(1)

Floridi L., Taddeo M., 2014. The Ethics of Information Warfare. Springer International Publishing Switzerland. DOI 10.1007/978-3-319-04135-3.

French National Digital Security Strategy, 2015. Available on the Internet: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/France_Cyber_Security_Strategy.pdf

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

Hiller J.S., Russel R.S., 2013. The challenge and imperative of private sector cybersecurity: An international comparison. Computer Law & Security Review, 29 (3): 236-245. Available on the Internet: <http://dx.doi.org/10.1016/j.clsr.2013.03.003>

Ignatavičius, R.; Tvaronavičienė, M.; Piccinetti, L. 2015. Sustainable development through technology transfer networks: case of Lithuania, *Journal of Security and Sustainability Issues* 4(3): 261-267. http://dx.doi.org/10.9770/jssi.2015.4.3(6)x

International Strategy for Cyberspace, 2011. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/international_strategy_for_cyberspace_US.pdf>

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

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

Kremer J. F., Muller B., 2014. Cyberspace and International Relations. Springer-Verlag Berlin Heidelberg.

Latvia‘s Cyber Security Strategy, 2014. Available on the Internet: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/lv-ncss

Laužikas, M.; Tindale, H.; Bilota, A.; Bielousovaitė, D. 2015. Contributions of sustainable start-up ecosystem to dynamics of start-up companies: the case of Lithuania, *Entrepreneurship and Sustainability Issues* 3(1): 8-24. http://dx.doi.org/10.9770/jesi.2015.3.1(1)

Min K.S., Chai S-W., Han M., 2015. An International Comparative Study on Cyber Security Strategy. International Journal on Security and Its Applications 9 (2): 13-20. Available on the Internet: <http://dx.doi.org/10.14257/ijsia.2015.9.2.02>

National Cyber Security Strategy, 2011, Ireland. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Luxembourg_Cyber_Security_strategy.pdf>

National Cyber Security Strategy, 2013, Hungary. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/HU_NCSS.pdf>

National Cybersecurity Strategy for Turkey, 2013. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cybersecurity-strategy-for-turkey/at_download/file>

National Cybersecurity Strategy II, 2015, Luxembourg. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Luxembourg_Cyber_Security_strategy.pdf>

National Strategic Framework for Cyberspace Security, 2013, Italy. Available on the Internet: <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/IT_NCSS.pdf>

NATO. 2011. Defending the networks: The NATO Policy on Cyber Defence. Available on the Internet: <https://ccdcoe.org/sites/default/files/documents/NATO-110608-CyberdefencePolicyExecSummary.pdf>

NATO. 2014. Wales Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. Press Release, 5 September, Available on the Internet: <http://www.nato.int/cps/en/natohq/official_texts_112964.htm>

NATO. 2015. Cybersecurity. November 25, 2015. Available on the Internet: <http://www.nato.int/cps/en/natohq/topics_78170.htm>

Natowatch. 2014. NATO Moves towards a ‘Cold War stand-off lite’: Defence Ministers Meetings in Brussels 3-4 June 2014. Briefing Paper No.52, 12 June. Available on the Internet: <http://natowatch.org/sites/default/files/briefing_paper_no.52_-_defence_ministers_meeting_june_2014.pdf>

Pauceanu, A. M. 2016. Innovation and entrepreneurship in Sultanate of 0man – an empirical study, *Entrepreneurship and Sustainability Issues* 4(1): 83-99. http://dx.doi.org/10.9770/jesi.2016.4.1(8)

Prause, G. 2016. E-Residency: a business platform for Industry 4.0?, *Entrepreneurship and Sustainability Issues* 3(3): 216-227. http://dx.doi.org/10.9770/jesi.2016.3.3(1)

Programme for the development of electronic information security (cyber security) Lithuania, 2011. Available on the Internet: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Lithuania_Cyber_Security_Strategy.pdf

Rezk, M. A.; Ibrahim, H. H.; Tvaronavičienė, M.; Sakr, M. M.; Piccinetti, L. 2015. Measuring innovations in Egypt: case of industry, *Entrepreneurship and Sustainability Issues* 3(1): 47-55. http://dx.doi.org/10.9770/jesi.2015.3.1(4)

Samašonok, K.; Išoraitė, M.; Leškienė-Hussey, B. 2016. The internet entrepreneurship: opportunities and problems, *Entrepreneurship and Sustainability Issues* 3(4): 329-349. http://dx.doi.org/10.9770/jesi.2016.3.4(3)

Segura Serrano A. 2015. Cybersecurity: towards a global standard in the protection of critical information infrastructures. EuropeanJournal of Law and Technology 6 (3). Available on the Internet: <http://ejlt.org/article/view/396/590>

Stahl W.M. 2007. The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity. Georgia Journal of International and Comparative Law 40: 247-273. Available on the Internet: <http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1024&context=gjicl>

The National Cyber Security Strategy Netherland, 2013. Available on the Internet: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf

Tvaronavičienė, A.; Žemaitaitienė, G.; Bilevičienė, T. 2016. Ecosystem for sustainable entrepreneurship: towards smart public procurement review procedures, *Entrepreneurship and Sustainability Issues* 4(1): 39-52. http://dx.doi.org/10.9770/jesi.2016.4.1(4)

Short biographical notes

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

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

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

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

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

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

Uldis Kinis. In 1981, Mr. Ķinis graduated the Faculty of Law of the University of Latvia. In 2006, Mr. Ķinis was conferred the doctoral degree in Law. Since July 2007 he was elected an associate professor of the Faculty of Law of the Riga Stradiņš University [Rīgas Stradiņa universitāte]. Uldis Kinis also is Vice-President of the Constitutional Court. He is the author of more than 30 publications mainly on problems of criminal law and information communications law.