Original Article

EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis

Darius Štitilis[a,*], Paulius Pakutinskas[b] and Inga Malinauskaitė[a]
[a]Business and Media School, Mykolas Romeris University, Ateities St. 20, 08303 Vilnius, Lithuania.
E-mail: stitilis@mruni.eu
E-mail: inga.malinauskaite@gmail.com
[b]Faculty of Law, Mykolas Romeris University, Ateities St. 20, 08303 Vilnius, Lithuania.
E-mail: paulius.pakutinskas@mruni.eu

*Corresponding author.

Abstract Given the global nature of cyber threats, assurance of a cyber security policy is very important not only at organization level but also at national level. Currently, cyber security as such is not independently regulated internationally; therefore the role of the EU and NATO in ensuring cyber security has become particularly significant. This article presents a study which compares the cyber security policies of the EU and NATO organizations. An analysis of how national cyber security strategies correspond with the cyber security policies and the strategic directions of these organizations has been carried out. We have also carried out a comparative study of the provision of national cyber security strategies of the EU and NATO. The study reveals that regardless of similar goals, namely assurance of cyber resilience, the selected harmonization and coordination approaches, as well as norms of national cybersecurity strategies, differ.
Security Journal (2017) **30**, 1151–1168. doi:10.1057/s41284-016-0083-9;
published online 17 October 2016

Keywords: cyber security strategies; regulation; comparative analysis; EU; NATO

Introduction

Cyber threat concerns have been expressed at different levels: internationally, regionally and at the national level. The number and frequency of cyber attacks in the EU states continue to increase. Carayannis *et al* (2014). The increasing number of cyber attacks has also been emphasized by international organizations such as NATO, which stated that repelling such attacks and protecting information systems has become one of its most important tasks (NATO, 2015).

In fact, people everywhere have searched for ways to protect information for a long time, even before the appearance of cyberspace. The application of information–communication technologies in the area of security in the broad sense started during World War I. The use of radio waves (radio telegraph) for sending and intercepting messages first

occurred during the First World War (BBC News, 2014). In 1914, British radio operators sent intercepted wireless signals from Germany to the Royal Navy radio intercept service. These in turn led to the setting up of Admiralty Room 40, where the messages were sent for cryptanalysis. This provided the foundation for the success of British intelligence during World War 1 (Lee, 1994). At the end of World War I, the German engineer Arthur Scherbius invented Enigma (Singh, 2011) – an electro-mechanical rotor cipher machine, which was developed and used in the early- to mid-twentieth century to protect commercial, diplomatic and military communication. This invention laid the basis for using calculators (something similar to modern computers) for security purposes. Alan Turing, the British scientist who created the calculator, invented a method for decoding messages encrypted by the Germans which were sent via open channels. This is how the information war was carried out and Germany itself suffered from the use of technologies, as its messages were intercepted and decoded, which gave the Allies a big advantage in defence and in safety in general.

We could say that the situation today is still very much the same, except that the measures, methods and technologies have changed. Cyber security and its assurance are also based on technology. In recent years, a number of international organizations, such as the International Telecommunications Union (ITU), NATO and the Organisation for Economic Cooperation and Development (OECD), have emphasized the importance of evaluation in cyber security policymaking (ENISA, 2014). The European Union can be distinguished among regional organizations. The EU and NATO, which have started coordinating and harmonizing the area of cyber security, can be distinguished as being the most active. Analysis of the cyber security activities of these organizations is also valuable, due to the fact that out of 33 countries in the general list, 28 countries are members of the EU and 28 countries are members of NATO. Thus, the majority of countries are members of both the union and the organization, and cybersecurity policy and strategy play an important role.

Realizing the emerging threats, the European Commission, together with the High Representative of the Union for Foreign Affairs and Security Policy, published a cybersecurity strategy (European Commission, 2013a). According to a press release issued by the European Commission, the strategy represents the EU's comprehensive vision on how best to prevent and respond to cyber disruptions and attacks. This action is meant to further the European values of freedom and democracy and to ensure that the digital economy can grow safely. Specific actions are aimed at enhancing the cyber resilience of information systems, reducing cybercrime and strengthening EU international cyber security policy and cyber defence (European Commission, 2013b) alongside a Commission-proposed directive on network and information security (NIS) (European Commission, 2013c). This Directive was approved by the European Parliament in July 2016. The aim of the Directive is to ensure a high common level of network and information security (NIS) across the EU (Directive, 2016/1148/EU). Ensuring NIS is vital to boosting trust and to the smooth functioning of the EU internal market. Regulatory obligations are required to create a level playing field and to close existing legislative loopholes (European Commission, 2013d). Provisions of the Directive will have to be implemented in individual EU states from 9 May 2018. Thus, coordination and harmonization of the EU cyber security area is initiated with the implementation of the following means: a draft

Directive, legally non-binding but a very important means of communication in practice and (in the future) a legally binding document – a Directive.

Meanwhile, the cyber security policy of NATO is formulated slightly differently. It should be noted that even though cyber security measures are not mentioned in the main North Atlantic Treaty, discussions have been held on whether this treaty obliges NATO members to take cyber defence measures in addition to traditional security measures. State representatives first officially asked for Article 5 of the North Atlantic Treaty to be used in a cyber attack in 2007, when Estonian public and private sectors were electronically attacked for several weeks by attacks from Russia (Stahl, 2007). Representatives of NATO member countries stated in 2014 that Article 5 of the North Atlantic Treaty on collective self-defence could be invoked in case of a cyber attack with effects comparable to those of a conventional armed attack (NATO, 2014).

Regarding specific actions of the Organization in forming cyber security policy, the issue of cyber defence was raised at the Prague Summit in 2002, in what was seen as a historic event (Carayannis *et al*, 2014). NATO Policy on Cyber Defence was published in 2011 (NATO, 2011). The new NATO Policy on Cyber Defence provides a solid foundation from which Allies can move forward in developing cyber security. The document clarifies both NATO's priorities and NATO's efforts in cyber defence – including which networks to protect and the way this can be achieved.

Another NATO document in the cyber security area was drawn up when the heads of state and governments of NATO member countries met in Newport, Wales, on 4–5 September 2014. Among other topics, they endorsed the Enhanced Cyber Defence Policy, which had already been approved by the defence ministers in Brussels on 3–4 June 2014. A synopsis of the Policy is provided by the Summit Declaration. According to the Policy, NATO recognizes that international law applies to cyberspace, and that cyber defence is part of NATO's core task of collective defence (CCDCOE, 2014). Thus, certain coordination of cyber security issues, even though undertaken in a legally non-binding way, namely, by representatives of NATO member countries approving cyber defence policy and issuing the Wales Summit Declaration (NATO, 2014), was also started at the NATO level.

In the cyber security context, clear development and publication of national cyber security strategies have been observed, particularly in the European Union, and this process has intensified since 2011. At the time of this research, out of 33 EU and NATO countries, 26 have already published national cyber security strategies (some strategies replaced previously valid strategies [previous strategies usually had different titles, for example, IT security strategy, etc.]). However, seven countries do not yet have such strategies (in some of these countries the strategies are being developed).

When it comes to national cyber security strategies, differences at the national level are always possible, and this may lead to the strategies themselves and their content being different; nevertheless, common strategy elements can be examined.

It should be noted that a number of studies have already compared the national cyber security strategies of EU countries (ENISA, 2014; BSA, 2015; Klimburg, 2012 and others). These studies revealed the similarities and differences of the strategies. However, the coordination initiatives of EU and NATO cyber security issues, and the provisions of cyber security strategies of individual countries have never been compared. Furthermore,

the strategic relations with cyber security strategies of the respective countries have not been determined.

Analysis of the said documents and the cyber security strategies of individual EU and NATO countries reveal the similarities and differences of such strategies, as well as the good practices which individual countries have developed at the national level.

Cyber Security Aims and the Policy and Strategy of the EU and NATO

The first moves towards strengthening the security of and trust in the information society started with a Commission proposal in 2001 (European Commission, 2001), and a strategy published in 2006 (European Commission, 2006) (Segura Serrano, 2015). The Cybersecurity Strategy of the European Union of 2013 (European Commission, 2013a) is considered to be the main strategic document of the EU in the cyber security field. The context for adoption of the strategy is associated with the increasing frequency of intentional and accidental cyber security incidents, and the issue of cybercrime adversely affecting the EU economy has been distinguished. The fight against cybercrime as one of three priorities has also been distinguished in the European Agenda on Security (European Commission, 2015). This agenda identifies cyber security as the first line of defence in fighting cybercrime. Thus, cybercrime can be considered one of the main issues targeted by EU authorities in the cyber security context. Meanwhile, NATO strategic cyber security provisions do not distinguish cybercrime as such, although the context is similar, the NATO strategic concept is related to the need to 'develop further our ability to prevent, detect, defend against and recover from cyber attacks…'.

A proposal in the EU cyber security strategy lays out the EU vision in this field, explaining tasks and competences, and listing actions which must be undertaken in order to firmly and effectively protect and strengthen the rights of citizens (European Commission, 2013a). Furthermore, the introduction of the strategy lists cyber security principles in accordance with which cyber security policy should be oriented in the EU and the world (European Commission, 2013a). Since one of the most important documents in the formation of cyber security policy is a national cyber security strategy, it can be stated that pursuant to the strategy, the respective principles should be provided for and implemented in specific national cyber security strategies.

NATO strategic provisions on cyber security are not laid out in such great detail. However, the main aspects are sufficiently and clearly distinguished: the context, main goals, principles, response, engagement of the international community and practical steps. As previously mentioned, not all strategic cyber security provisions are structured – the Wales Summit Declaration contains two paragraphs on cyber security, without a more detailed structure.

Even though the content is not examined due to the limitations of this study, the following principles are enshrined in the EU strategy.

– The EU's core values apply as much in the digital as in the physical world.
– Protecting fundamental rights, freedom of expression, personal data and privacy.
– Access for all.

 © 2016 Macmillan Publishers Ltd. 0955-1662 **Security Journal** Vol. 30, 4, 1151–1168

– Democratic and efficient multi-stakeholder governance.
– A shared responsibility to ensure security.

At the principle level, NATO does not classify cyber security principles as clearly as the EU strategy does. However, it does distinguish that NATO cyber defence efforts are based on the overarching principles of prevention, resilience and non-duplication. Prevention and resilience are particularly important given the reality that certain threats will persist despite all efforts to protect and defend against them. Preventing such attacks from occurring in the first place will be achieved by increasing our level of preparedness and mitigating risk by limiting disruptions and their consequences. Resilience is a key because it facilitates rapid recovery in the aftermath of an attack (NATO, 2011). Even though presented differently, the principles declared by the EU and NATO are relevant and can even complement each other. The unique principle of non-duplication is important in ensuring synergy between the EU and NATO in the pursuit of cyber resilience. The importance of this principle has recently increased because people have begun to realize that joint employment of military forces and civil resources for protection can help make it much 'smarter' and more efficient (Carayannis *et al*, 2014). This principle should also be followed in the coordination of cyber security issues at the national level.

The main focus of the EU strategy is on specific actions which could increase the overall results achieved by the EU. These actions are both short and long term: they include a variety of policy tools and involve different types of actors, be it the EU institutions, Member States or industry. The EU vision presented in this strategy is articulated in five strategic priorities which address the challenges highlighted above (European Commission, 2013a):

1. Achieving cyber resilience.
2. Drastically reducing cybercrime.
3. Developing cyber defence policy and capabilities related to the Common Security and Defence Policy.
4. Developing the industrial and technological resources for cybersecurity.
5. Establishing a coherent international cyberspace policy for the European Union and promote core EU values.

NATO's strategic cyber security provisions do not distinguish strategic priorities as clearly as the EU strategy does. An examination of the goals clearly reveals that this is a military organization with more limited goals than the EU. According to the cyber defence policy of NATO:

> 'NATO will implement a coordinated approach to cyber defence that encompasses planning and capability development aspects in addition to response mechanisms in the event of a cyber attack. To achieve this, NATO will incorporate and integrate cyber defence measures across all Alliance missions. For cyber defence capability development, the NATO Defence Planning Process (NDPP) will guide the integration of cyber defence into national defence frameworks. Recognising that NATO requires a secure infrastructure upon which it can operate, NATO networks, including NATO agencies and NATO missions abroad, will be brought under centralised protection.

> NATO will also develop minimum requirements for those national networks that are connected to or process NATO information. To achieve this, NATO will identify its critical dependencies on the Allies' national information systems and networks and will work with Allies to develop minimum cyber defence requirements. NATO requires a secure infrastructure on which it can operate, therefore it is important that Allies ensure the protection and defence of national critical information systems and networks. If requested, NATO will assist Allies in achieving a minimum level of national cyber defence.' (NATO, 2011).

Thus, NATO concentrates more on more internal organization priorities.

In this article, only those priorities whose implementation are relevant (or may be implemented) in national cyber security strategies according to the EU strategy will be distinguished for further comparative analysis.

The strategic priority 'Achieving cyber security' emphasizes cooperation with the private sector in pursuit of cyber resilience. Cyberspace is mostly controlled and operated by the private sector and thus cooperation between the public and private sectors is essential in order to properly respond to current threats aimed at cyberspace (Min *et al*, 2015). Cooperation with the private sector is also important because of the prevailing common understanding that governments cannot ensure the necessary cyber security level without involving the private sector. However, there are still discussions on how exactly the private sector should be involved (Tropina and Callanan, 2015). The private sector can no longer stand on the side-lines and wait for laws against cybercrime and computer intrusions to be enforced. Their own self-interest and the interest of the networked environment demand their vigilance (Hiller and Russel, 2013). As indicated in the strategy, there are still EU-wide gaps regarding the participation and preparedness of the private sector (European Commission, 2013a). Fostering a culture of cyber security, which could expand business opportunities and increase competitiveness in the private sector, is also mentioned. Cyber incident trainings, which must involve the private sector, are also important in this context.

NATO also emphasizes cooperation with the private sector, indicating that technology innovation and expertise from the private sector are of critical importance. Cooperation with industry was also emphasized at the NATO Defence Ministers Meeting in Brussels in 2014 (Natowatch, 2014).

Increasing awareness of end users in the area of cyber security is distinguished as a second aspect, in addition to cooperation with the private sector. In the strategy, the Commission suggests having a 'cyber security month' in cooperation with the private sector and increasing national efforts, providing educational and vocational training on TIS-related issues (education in schools, training computer students on the protection of personal data, basic training of public administration employees). Even though understood in a narrower sense, training and the development of competence have also been distinguished in NATO strategic documents.

One of the most important strategic EU priorities is a reduction in the number of cyber attacks, and the strategy has identified strict and efficient laws as one of the most important measures to achieve this (European Commission, 2013a). Even though the Convention on Cybercrime (Council of Europe, 2001) was adopted in 2001, to this day only 47 countries have ratified the convention (Council of Europe, 2016), and the total number of countries

ranges from 189 to 196 countries according to different sources (Worldatlas, 2016). Some EU and NATO countries have not ratified this convention (Council of Europe, 2016). The EU has adopted legislation on cybercrime, including the directive on combating the sexual exploitation of children online and child pornography (Directive, 2011/92/EU), and the directive on attacks against information systems (Directive, 2013/40/EU). However, provisions of the Convention are broader in terms of both substantive and procedural law as well as in other aspects (international cooperation, etc.), thus the Convention still plays an important role, and its ratification among other countries is essential in the fight against cybercrime. The strategy also encourages Member States that have not ratified the Budapest Convention on Cybercrime to ratify it as soon as possible and to implement its provisions. National strategies emphasize the necessity for strict and efficient legislation in fighting cybercrime. National cyber security strategies of the countries which have still not ratified the convention should make the ratification of this convention one of their top goals.

NATO does not distinguish the fight against cybercrime as such, but instead it sets goals to protect networks and critical resources. Thus, NATO focuses on protection itself and on cyber defence rather than focusing on reasons: for example, how to reduce the number of cybercrimes and the threat which they pose. Such a stance is believed to be more related to the purpose of NATO itself.

Another very important priority in the strategy of 2013 is the development of cyber defence policy, and capabilities related to the framework of the Common Security and Defence Policy. To increase the resilience of the communication and information systems supporting Member States' defence and national security interests, cyber defence capability development should concentrate on detection, response and recovery from sophisticated cyber threats. It is noteworthy that NATO bases most of its activities related to cyberspace on cyber defence.

Given that threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be enhanced. These efforts should be supported by research and development and closer cooperation between governments, the private sector and academia in the EU. To avoid duplications, the EU will explore opportunities on how the EU and NATO can complement their efforts to heighten the resilience of critical governmental, defence and other information infrastructures on which the members of both organizations depend (European Commission, 2013a). Protection of critical infrastructure is identified as one of the key comprehensive cyber security strategy elements (Kremer and Muller, 2014), and the regulation of this category should only intensify (Segura Serrano, 2015). To this end, the European Commission initiated the adoption of the Network and Information Security Directive; the main purpose of which is to establish requirements for managers of such infrastructure (European Commission, 2013a). It is believed that EU and NATO (i.e. civilian and military) synergy in cyber security should also be discussed in national cyber security strategies. Scientific research and protection of infrastructure of exceptional significance have been identified as some methods of synergy.

Scientific research has also been encouraged in another priority – development of industrial and technological resources aimed at cyber security. In addition to the promotion of research, the achievement of this priority is associated with the marking of security, adoption of security standards and the application of voluntary certification schemes. All

these marking/standard measures can be described as self-regulation measures, which are also very important in ensuring cyber security.

Support for EU fundamental values has been emphasized in the priority 'creating consistent EU international cyber policy and supporting EU fundamental values'. One of the most important elements of EU international cyber policy will be to promote cyberspace as an area of freedom and fundamental rights (including access to information and freedom of expression). Expanding access to the internet should advance democratic reform and its promotion worldwide. Increased global connectivity should not be accompanied by censorship or mass surveillance. The EU should promote corporate social responsibility (European Commission, 2013a). NATO as a military organization does not mention these values in its cyber security strategic provisions, but it indicates in common declarations that: 'We stand ready to act together and decisively to defend freedom and our shared values of individual liberty, human rights, democracy, and the rule of law' (NATO, 2014).

In addition to the priorities, the strategy of 2013 distinguishes 'tasks and competence'. The issue of inter-institutional coordination is relevant at the national level. Member States should have, either already or as a result of this strategy, structures to deal with cyber resilience, cybercrime and defence, and they should achieve the required level of capability to deal with cyber incidents. However, given that a number of entities may have operational responsibilities over different dimensions of cyber security, and given the importance of involving the private sector, coordination at the national level should be optimized across ministries. Member States should set out in their national cyber security strategies the roles and responsibilities of their various national entities (European Commission, 2013a). NATO strategic documents do not deal with issues of tasks and competence.

Cyber defence is believed to have become the main NATO policy (Carayannis *et al*, 2014) which will lead to increased significance of NATO strategic provisions on cyber security. It is believed that NATO should expand the scope of its cyber security policy and itemize it, resolving issues related to cooperation with other organizations and the private sector, as well as other issues.

In summary, the following selected criteria in the examination of provisions of national cyber security strategies of EU and NATO countries can be distinguished: principles, cooperation with the private sector, the fight against cybercrime, cyber defence, scientific research, standards and support of fundamental values. One additional criterion, namely, provisions regarding tasks and competence of 'players'/institutions, will be also used, even though NATO cyber security strategic documents do not contain these provisions.

Comparison of National Cyber Security Strategies of EU and NATO Countries in Relation to EU and NATO Cyber Security Strategies

A comparison of national cyber security strategies of EU and NATO countries was conducted by comparing the main criteria[1] in the latest valid cyber security strategies of the respective countries. It should be noted that the cyber security strategies of all the compared countries are from 2010 and later. Thus, it can be stated that strategies adopted during the past four years have been evaluated. Certain countries readopted their cyber

security strategies, while some countries adopted strategies for the first time. The majority of countries specify the year of adoption in their strategies, but do not indicate the specific validity period of the strategies, which means that the currently valid strategy will be valid until the adoption of a new one. However, some countries (such as Estonia, Ireland and Latvia) indicate the validity period of their strategies, which is usually two years, in the strategy itself. The Lithuanian programme can be distinguished in this context – the validity period of the strategy is eight years, namely, from 2011 to 2019. It is generally believed that countries should draw up strategies in a field as dynamic as cyber security for no longer than a few years.

When comparing strategic provisions in terms of their principles, 11 countries[2] do not have separately distinguished cyber security principles in their national cyber security strategies. Cyber security principles have not been distinguished in strategies which are completely new, i.e. adopted in 2015 (those of Denmark, France and Luxembourg). The provisions of strategies of countries whose national cyber security strategies do not distinguish cyber security principles, also contain differences; there are countries[3] with cyber security strategies which do not clearly specify a single principle. However, following single principles can be noticed in the provisions of strategies of other countries: responsibility (Albania, Norway), the principle of Fundamental Law and the principle based on the review of relevant values and interests (Hungary), the principle of supported democratic values (Italy), the principle of collective security and one-stop shop (Lithuania) and the principles of proportionality and necessity (Luxemburg).

However, 18 countries do have separately distinguished principles. The principles in the strategies of all countries differ in number, title and content. Some countries have three principles (Ireland), while others have 13 (Turkey). Among those 18 countries, there is not a single country for which the principles presented in the national cyber security strategy completely match the principles declared in the EU and NATO cyber security strategies. However, the principles of the mentioned countries have certain similarities: principles of proportionality, cooperation, the rule of law, responsibility, fundamental rights and freedoms, risk management and an integrated approach are often distinguished. However, the differences are greater than the similarities: certain countries divide principles into groups, in the strategies of other countries, the principles themselves have specific subparts, or unique principles are presented (such as the use of national products and services [Turkey], increasing cyber force [the Czech Republic]). The greatest number of differences has been observed between the provisions of the cyber security strategies of NATO countries which are not members of the EU: Albania, Canada and Norway do not have separately distinguished principles, Turkey has 13 principles (similar to those of the European countries), while the US has three distinctive cyber security principles: fundamental freedoms, privacy and the free flow of information. Thus, the presentation of principles in national cyber security strategies of the examined countries can be stated to have no unified system and, despite some similarities, the principles differ.

When it comes to cooperation with the private sector, the situation here is the best compared to all the examined criteria in the national cyber security strategies. It could be said that two countries (Lithuania and Poland) are not promoting cooperation with the private sector and do not distinguish it clearly as a pursuit or a measure. Nevertheless, it would be wrong to say that Lithuania and Poland do not mention cooperation with the private sector at all. The Lithuanian cyber security programme mentions the lack of

cooperation between the public and the private sector, while the Polish cyber security strategy mentions cooperation with entrepreneurs, which can be considered one element of cooperation with the private sector.

Distinguishing cooperation with the private sector in national strategies is considered to be an important measure for ensuring cyber security, and is directly referred to as one of the main goals in certain national strategies. However, it should be noted that despite cooperation with the private sector being declared in national cyber security strategies of certain countries (Belgium, the Czech Republic, Italy, Latvia), reviews performed by BSA (BSA, 2015) show that in practice, these countries[4] do not have sector-specific joint public–private plans or defined public–private partnerships in place. Thus, regardless of the fact that it has been mentioned in the cyber security strategy, a declared partnership with the private sector still has to be implemented in practice. Italy, which declared cooperation with the private sector in its strategy of 2013 – drawing up a separate strategy part on PPP – can be distinguished. Also, this study reveals that user awareness-raising and training have been indicated and described in the national cyber security strategies of the majority of the selected countries, but only as separate measures rather than in the context of cooperation with the private sector.

National cyber security strategies of seven countries do not directly mention the fight against cybercrime and the reduction of the number of cybercrimes, while the strategies of the remaining countries distinguish the fight against cybercrime and the reduction of the number of cybercrimes as a goal, a guideline, a challenge or a principle. It often happens that national strategies have a separate strategy chapter on fighting cybercrime or reducing the number thereof, discussing the issue and possible measures in greater detail. When it comes to the examined countries, the national cyber security strategy of the only country which has not ratified the Convention on Cybercrime, namely, Ireland, also distinguishes the fight against cybercrime. Cases of when a fight against cybercrime is directly related to the capabilities of law enforcement institutions to detect and investigate cybercrime have been observed; thus in such cases, the necessity to increase law enforcement capacities and capabilities in the respective area is emphasized.

The strategies of countries where the fight against cybercrime has been distinguished separately often advocate for legislation to combat cybercrime. This can be related to liability for cybercrime or advocated in a broader context, expanding to improvement of the cyber security category legal environment. However, it should be mentioned that the strategies of six countries do not mention legislation. All these countries have ratified the Convention on Cybercrime. Meanwhile, the strategy of the only country which has not ratified the Convention, Ireland, emphasizes the necessity of the appropriate legal environment with regard to cybercrime, associating such legal environment mainly with Directive No. 2013/40/ES on attacks against information systems.

This comparative study also showed that the provisions of national cyber security strategies on cyber defence and capabilities are significantly different. Twelve national cyber security strategies do not separately distinguish issues of cyber defence and capabilities. Only some of these countries mention aspects of resilience, which is considered to be only one of the elements of cyber defence [cyber defence: preparation, response and recovery (Klimburg, 2012)]. Countries which separately distinguish cyber defence single out these issues as one of the goals and pillars. In the context of cyber defence, Belgium, Czech Republic, Estonia, Hungary, the Netherlands and Spain mention

cooperation with NATO, including collective defence. Thus, these countries consider cooperation with NATO to be one of the main elements ensuring cyber security. In the evaluation of the strategies of all examined countries, cooperation with NATO is mentioned quite often, but not always in the context of cyber defence. However, there are also examples such as Norway – a NATO member – which does not mention this Organization in its national cyber security strategy. Furthermore, national strategies often mention critical infrastructure and its protection, but not always through the aspect of cyber defence. Germany can be mentioned as an example because its strategy lists specific sectors of critical infrastructure. However, this is an exception. In certain cases, national strategies of certain countries devote a special part to critical infrastructure and/or present a concept of critical infrastructure.

Scientific research and general research on cyber security are not mentioned in five national security strategies. Thus, it can be stated that research is emphasized in one way or another in the strategies of the remaining countries. However, the standards of the strategies of these countries contain differences. One group of countries emphasizes applied cyber security research, research and development (in general) or research in funded projects. Another group of countries distinguishes cooperation with universities and other academic institutions without emphasizing scientific research as such; the strategies of only a few countries (such as Croatia, the Netherlands and Spain) directly refer to scientific research and the necessity for it in the cyber security area.

The application of standards in the area of cyber security is mentioned in the national strategies of 13 countries, while the strategies of the remaining countries do not discuss this aspect. The practice of mentioning standards in strategies differs: in certain cases international standards are mentioned, others mention security standards, and others mention technical and other standards. Usually, the provisions do not specify any great detail, and in those rare cases where they are detailed, this is done indicating that standards must apply for the protection of critical infrastructure or in the public sector. In special cases, typical security standards and their assurance are associated with NATO (Germany). Marking is hardly mentioned at all in the national cyber security strategies of the analysed countries.

A comparison of provisions on the support of fundamental values/human rights in national cyber security strategies has shown that the provisions of countries (a majority) which mention them are of a broader nature (related to human rights) or a narrower nature, perceived as support of privacy only. These values are often declared as one of the principles. However, the strategies of eight countries[5] do not emphasize or mention support of fundamental values/human rights, which is considered a rather large number in light of the fact that consideration and respect for human rights is very important in assuring cyber security. Of course, a certain balance between privacy and security must be ensured. This is mentioned in, for example, the UK strategy, which provides one of the principles: balancing security with freedom and privacy. It is noteworthy that the Netherlands and Norway distinguish an important principle of privacy by design in the context of support for human rights, in accordance with which newly created products, services or new processes must also be evaluated in the context of privacy protection. For example, in Norway, prior to implementing new measures, a privacy impact assessment must be conducted and, if necessary, the Norwegian Data Protection Authority should be involved in planning and implementation (Cybersecurity Strategy for Norway, 2012).

Even though issues of tasks and competences of national institutions and other involved sectors in the area of cyber security are discussed solely in the EU cyber security strategy, this criterion has also been included in the comparative study of national cyber security strategies. The results obtained reveal that the national cyber security strategies of most of the countries do not solve the issues of 'tasks and competence', and only seven countries mention this aspect in their strategies. In the majority of cases (Albania, Cyprus, Italy, Latvia, Norway and Spain), the cyber security organizational structure with functions and responsibilities is presented. The strategy of Cyprus does not mention institutional functions, while structure in the Latvian strategy is understood as a measure for implementing the strategy. However, this strategy presents the visualization of the organizational structure. The strategy of Austria does not have a complete organizational structure; more attention is devoted to CERT and steering group functions. It should be noted that in all cases, most often the structure of the public sector is presented, and too little attention is paid to functions of the private sector and responsibilities ensuring cyber security.

In the evaluation of differences between national cyber security strategies to the extent they are related to the examined criteria, if a country is solely a member of the EU or NATO, no essential differences with regard to dependence have been observed. Here, the US cyber security strategy, where the impact of the so-called 'Bush Doctrine' – mainly formulated after the September 2011 events – clearly stands out. The broad mandate of the Bush Doctrine effectively makes the idea of 'global safekeeping' an important part of a national security strategy, giving the United States an open-ended unilateral license to respond militarily, in the name of the 'war on terror', to any acts or events in the world based solely on the internal perception of the United States (Floridi and Taddeo, 2014). However, this peculiarity is not directly impacted by US membership of NATO, but rather by a position formed inside the US.

The following countries have national cyber security strategies that are in line with the most criteria: Estonia, Italy, Latvia, Spain (compliance with all the criteria), United Kingdom and the USA. Does this mean that these countries are the best at ensuring cyber security? Yes, a cyber security strategy is one of the main measures for ensuring cyber security, but it is not the only one. A strategy is only a certain guide in the achievement of a goal, one of the bases on which cyber security should be created in the country. Thus, those countries with strategies that solve key issues comprehensively have a better tool for further work in ensuring cyber security and can be demonstrated as examples. For instance, the Estonian strategy serves as an example for Georgia as well as other states, and is regarded as an example of good practice for cyber security strategy within the wider Central and Eastern Europe region (Cybercrime and cybersecurity strategies, 2014).

Furthermore, it should be mentioned that when examining strategic provisions, the importance of the legal environment in ensuring cyber security has often been emphasized in strategies. In certain cases, the legal environment is understood in a narrower sense (for example, it is related to cybercrime and the protection of personal data), while in other cases it is perceived more broadly, to the extent related to cyber security. In any case, cyber security strategies can also be stated to have a great impact on the respective legal environment in the cyber security area, and thus certain provisions of these strategic documents may be assessed as preparatory and initiating respective legislative processes. Compilers should therefore take this into account when drawing up strategies.

Unified National Cyber Security Strategies of EU and NATO Countries

The EU cyber security strategy is an integral well-structured document aimed at providing a unified vision of the EU's assurance of cyber security and the indirect impact of documents on the cyber security of EU Member States. The main goal of NATO is defence, and cyber defence has become a part of this. Several documents or parts of them were released, so as to ensure this goal. However, compared to the EU cyber security strategy, the scope of issues which they cover is narrower and the provisions are not particularly detailed. Strategic documents of the EU and NATO in the area of cyber security can be stated to differ in their form, structure and scope. Even though the cyber security strategy of NATO is still under formation, its significance will increase, and cyber security is likely to become a key NATO policy. Despite the differences, both organizations declare that assurance of cyber security is a priority, and there are a number of similarities.

In light of the policies of the two organizations in the area of cyber security, cyber security strategies should reflect these policies at the national level. Our investigation showed that there are similarities and synergies between national cyber security strategies, and that they reproduce the cyber security policy of the EU and NATO in certain aspects. In summary, the following similarities were identified according to some criteria:

- Strategies of most of the countries (18) distinguish their principles. The following principles recur most often: principles of proportionality, cooperation, the rules of law, responsibility, fundamental rights and freedoms, risk management and an integrated approach.
- Most countries mention cooperation.
- Usually the fight against cybercrime or the reduction of the number of such crimes is distinguished in national strategies as a separate goal, guideline, challenge or principle. The strategies of those countries where a fight against cybercrime has been distinguished separately often advocate for legal measures in the fight against this phenomenon.
- Scientific and general research is mentioned in most of the countries.
- Standard-related issues are solved in the strategies of 13 countries.
- More than two-thirds of the countries emphasize support for human rights.

However, fundamental differences were observed according to other criteria, and there are more differences than similarities or synergies. The following is a summary of the differences observed:

- Principles in national strategies are presented differently, and their number differs as well. Principles are not presented in a unified way. Less than half of the countries examined distinguish principles at all in their strategies.
- Provisions on cooperation are not detailed in the majority of cases. Not all the countries have implemented partnership with the private sector in practice, and the provisions of some countries (such as Italy, Luxembourg and Romania) still remain of a more declarative nature. Consumer awareness, awareness-raising and training is not done in the context of cooperation with the private sector.

- Provisions of national strategies on cyber defence and capabilities differ significantly. Twelve countries do not distinguish these issues, while those that do distinguish them present them as one of the goals or key pillars. Six countries mention cooperation with NATO in the context of cyber defence. Overall, cooperation with NATO is often mentioned in the strategies of the examined countries as an important element, but not always in the context of cyber defence. Furthermore, strategies often mention the protection of critical infrastructure, but not always through the cyber defence aspect.
- Scientific and general research is not mentioned in the strategies of five countries. Those strategies which do mention it present research in a different context: either associating it with funded research, in cooperation with universities or with the necessity for scientific research (in three countries only).
- Standard-related issues are solved very differently: mentioning international, general security or technical standards, without itemizing them. Meanwhile, strategies which itemize them usually associate the application of standards with critical infrastructure or the state sector. And the strategies merely deal with marking issues. Standard-related issues are not solved at all in more than half of the countries.
- The strategies of eight countries do not emphasize support for human rights. Strategies of countries which mention this issue declare values in a broader or narrower sense (as support of privacy).
- More than two-thirds of countries do not mention "player" functions and competences in their strategies.

The differences in national cyber security strategies themselves raise additional questions. For example, in a significant number of countries, principles are not distinguished at all. This can mean that strategies of respective countries focus more on details, but lack conceptual and essential elements such as principles, bases of cyber defence, etc. Perhaps this is another reason why it is difficult for some countries to have long-term cyber security strategies; since details change rapidly and with the lack of conceptual elements, strategies need to be changed more often. Differences in cooperation have also been observed. Such differences were not expected, because cooperation is classically applicable in various fields. In particular, differences in the area of cyber defence can be distinguished. How can a common resilience level be expected when the solution of cyber defence issues differs so greatly at the national level? This shows the need to unify national strategies.

Consequently, it is obvious that there are many more differences and discrepancies than similarities between national cyber security strategies according to the selected criteria; this is seen as an impediment to the pursuit of a common cyber security policy. Achieving the desired unification with the help of the EU cyber security strategy and NIS Directive is very unlikely. On the one hand, the EU documents are only applicable within the EU, while one of the mentioned documents – 'the strategy' – is optional. On the other hand, when it comes to the analysis of the provisions of the aforementioned EU documents, they are too abstract. Article 7 of the Directive lists things that must be provided within the national cyber security strategy (for example, an indication of education). However, these provisions do not indicate the level of specifics and detail of reflection of the issues in strategies, i.e. unification of the content itself is not pursued. The Directive does provide for the fact that Member States may request the assistance of ENISA in developing national strategies on the security of network

and information systems[6] but considering the fact that the Directive will take effect only 21 months after its adoption (9 May 2018), unification may take longer.

One of the ways to unify national cyber security strategies could be the proposal of a national cyber security strategy model. However, in such a case, other minor questions arise: whether the same unified strategy model is possible and to what extent, whether certain parts of strategies should be different, what determines such differences or how could national characteristics be reflected in national cyber security strategies? Consideration should also be given to whether essential national characteristics and local interests can exist together in the presence of a common electronic space. All these questions are the subjects of further research.

Conclusion

It should be noted that the EU and NATO cyber security strategic documents differ in both the scope and aspects emphasized. However, solving these common issues shows that the approach of the EU and NATO to cyber incidents and the fight against it is similar. Thus, it is essentially possible to have a synergy of approaches in the different countries when adopting, updating or amending provisions of national cyber security strategies in order to ensure cyber security.

Strategic cyber security documents of both the EU and NATO (as organizations) distinguish general issues, and these were used in the comparative study as selected criteria when examining the provisions of national cyber security strategies of EU and NATO countries: principles, cooperation with the private sector, the fight against cybercrime, cyber defence, scientific research, standards and support of fundamental values.

Having conducted research according to the mentioned criteria, a number of similarities were found. However, there were many more differences or discrepancies between national cyber security strategies according to the selected criteria. The main differences include different principles, provisions on cooperation, cyber defence, research, application of standards, protection of human rights, 'player' functions and competences. Differences mean that in certain cases not only do provisions differ, but they can be absent altogether. These differences also show that national countries were the first to start developing national cyber security strategies, while documents of the EU and NATO as organizations obviously had no impact on the content of these strategies at all. Even though additional studies on cyber security strategies were conducted, for now there is a lack of specific actions, especially on the part of NATO, coordinating the implementation of studies in practice.

These differences in national cyber security strategies are believed to interfere with the achievement of a unified cyber security policy at the national level. Since all strategies are still very different, further coordination with the help of a network and information security directive and other possible legal instruments is necessary, particularly as cyber security has become a global issue. The preparation and proposal of a unified national cyber security strategy model could be a separate additional proposal. Such a proposal would help to better ensure a common cyber security policy at the regional organizational (EU and NATO) level and raise cyber security culture as evenly as possible.

Producing a unified national cyber security strategy model could be impacted by the fact that differences in national characteristics, which should be reflected in strategies, should not

be rejected. On the other hand, the proposal of a unified national cyber security strategy model could have a positive impact on unifying the provisions of cyber security strategies. Currently, this cannot be ensured either by current legislation or by other EU and NATO documentation.

It may still be too early to create a specific unified national cyber security strategy model (a uniform document) applicable to all countries. However, discussions or considerations that take the cyber security strategies of those countries that are most advanced in the area of cyber security as an example, should at least be started. Perhaps a few unified strategy models could be created depending on the size of the country or other criteria. As NATO CCDCOE has developed a number of documents, it could be the organization in charge of coordinating further research and discussions or consideration, especially in light of the fact that no essential differences were observed between the strategies of NATO and EU countries, while the existing ones (such as those of the USA) were the result of other factors rather than of membership in these organizations.

Estonia, Italy, Latvia, Spain, UK and the USA met the most examined criteria. These countries have a better tool for ensuring cyber security and this also directly impacts the respective legal environment. The cyber security strategies of these countries, as well as of others that are considered most advanced in the area of cyber security according to different criteria, could be used as examples to develop a typical national cyber security strategy model. The interest of all the countries in having such a model is huge. Being of global nature, the cyber security area itself creates preconditions for the formation of such a unified model or models.

Acknowledgement

This research was funded by a grant (No. MIP-099/2015/PRC-36) from the Research Council of Lithuania.

Notes

1 In summary: (1) principles, (2) cooperation with private sector, (3) the fight against cybercrime, (4) cyber defence, (5) research, (6) standards, (7) support of fundamental values, (8) tasks and competence of "players"/ authorities.
2 National cyber security strategies which do not distinguish cyber security principles: Albania, Belgium, Canada, Denmark, France, Hungary, Italy, Lithuania, Luxembourg, the Netherlands, Norway.
3 National cyber security strategies which mention not a single cyber security principle: Belgium, Canada, Denmark, France, the Netherlands.
4 Albania, Belgium, Canada, Denmark, France, Hungary, Italy, Lithuania, Luxemburg, Netherlands, Norway.
5 Albania, Belgium, Cyprus, Denmark, Germany, Hungary, Luxemburg, Poland.
6 Article 7(2) of the Directive.

References

'Cybercrime and cybersecurity strategies in the Eastern Partnership region. Results of a regional workshop', Chisinau, Republic of Moldova, 12–14 November 2014, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803053d2, accessed 1 February 2016.

BBC News (2014) World War One: How radio crackled into life in conflict, (Charlotte Dubenskij. 18 June 2014), http://www.bbc.com/news/uk-wales-27894944, accessed 4 July 2016.

BSA. (2015) EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace, http://cybersecurity.bsa.org/index.html, accessed 1 February 2016.

Carayannis, E., Campbel, D. and Efthymiopoulos, M. (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, http://ccdcoe.org/nato-summit-updates-cyber-defence-policy.html, accessed 1 February 2016.

Council of Europe (2001) 'Convention on Cybercrime, Budapest', No. 185, 23 November, http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561, accessed 1 February 2016.

Council of Europe (2016) Chart of signatures and ratifications of Treaty 185, http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=P60tWvz9, accessed 1 February 2016.

Cybersecurity Strategy for Norway (2012) https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Norway_Cyber_Security_StrategyNO.pdf, accessed 1 February 2016.

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:335:0001:0014:EN:PDF, accessed 1 February 2016.

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, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:en:PDF, accessed February 1, 2016.

Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN, accessed 10 August 2016.

ENISA. (2014) An Evaluation Framework for National Cybersecurity Strategies. November 2014, https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies/at_download/fullReport, accessed 1 February 2016.

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, https://ccdcoe.org/sites/default/files/documents/EU-010606-NISProposal.pdf, 1 accessed February 2016.

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, http://ec.europa.eu/information_society/doc/com2006251.pdf, accessed 1 February 2016.

European Commission (2013a) 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, 7 February. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667, accessed 1, February 2016.

European Commission (2013b) 'EU Cybersecurity plan to protect open internet and online freedom and opportunity', Press Release, 7 February, http://europa.eu/rapid/press-release_IP-13-94_en.htm, Accessed 1 February 2016.

European Commission (2013c) 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, 7 February, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666, accessed 1 February 2016.

European Commission (2013d) Commission Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, 7 February, http://ec.europa.eu/digital-agenda/en/news/commission-proposal-directive-concerning-measures-ensure-high-common-level-network-and, accessed 1 February 2016.

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, http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf, accessed 1 February 2016.

Floridi, L. and Taddeo, M. (2014). *The Ethics of Information Warfare*. New York: Springer International Publishing. doi:10.1007/978-3-319-04135-3.

Hiller, J. and Russel, R. (2013) The challenge and imperative of private sector cybersecurity: An international comparison, *Computer Law & Security Review* 29(3): 236–245. 10.1016/j.clsr.2013.03.003, accessed 1 February 2016.

Klimburg, A. (2012). *NATO cybersecurity framework manual*. Tallinn: NATO CCD COE Publication, NATO Cooperative Cyber Defence Centre of Excellence.

Kremer, J. and Muller, B. (2014). *Cyberspace and International Relations*. Berlin: Springer.

Lee, B. (1994) Radio Intelligence Developments during World War One and Between the Wars, California Historical Radio Society, http://antiqueradios.com/chrs/journal/intelligence.html.

Min, K., Chai, S.-W., and Han, M. (2015) An International Comparative Study on Cyber Security Strategy. *International Journal on Security and Its Applications* 9(2): 13–20. 10.14257/ijsia.2015.9.2.02, accessed 1 February 2016.

NATO (2011) Defending the networks: The NATO Policy on Cyber Defence, https://ccdcoe.org/sites/default/files/documents/NATO-110608-CyberdefencePolicyExecSummary.pdf, accessed 1 February 2016.

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, http://www.nato.int/cps/en/natohq/official_texts_112964.htm, accessed 1 February 2016.

NATO (2015) Cybersecurity, 25 November 2015, http://www.nato.int/cps/en/natohq/topics_78170.htm, accessed 1 February 2016.

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, http://natowatch.org/sites/default/files/briefing_paper_no.52_-_defence_ministers_meeting_june_2014.pdf, accessed 1 February 2016.

Segura Serrano, A. (2015) Cybersecurity: towards a global standard in the protection of critical information infrastructures. *European Journal of Law and Technology* 6(3), http://ejlt.org/article/view/396/590, accessed 1 February 2016.

Singh, S. (2011). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. New York: Knopf Doubleday Publishing Group. ISBN 978-0-307-78784-2.

Stahl, W. (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, http://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1024&context=gjicl, accessed 1 February 2016.

Tropina, T.and Callanan, C. (2015). *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*. New York: Springer International Publishing.

Worldatlas (2016) How Many Countries are in the World? http://www.worldatlas.com/nations.htm, accessed 1 February 2016.