Information & Security: An International Journal

Aleksandar Klaic, v.34:1, 2016, 37-55 https://doi.org/10.11610/isij.3403

A METHOD FOR THE DEVELOPMENT OF CYBER SECURITY STRATEGIES

Aleksandar KLAIC

Abstract: Cyberspace has become an intrinsic part of today's society by creating a distinct virtual dimension in its functioning. Nations and the international community invest significant efforts to assure certain terms and responsibilities in this virtual dimension. The elaboration of national, NATO and EU cyber security strategies in a very short time received a high priority. The questions about the responsible institutions assigned in the strategies, guiding principles to follow, and the way of implementation are approached differently by different nations. The goal of this article is to propose a method that offers a more consistent approach to the development of cyber security strategies. The key research question is whether the proposed approach results in a more consistent national cyber security strategy that covers all the necessary national requirements and expectations, and thus makes it easier to harmonise with the variety of international requirements. In order to verify the proposed method, the article presents a brief overview of the results achieved in the case of the development process of Croatia's National Cyber Security Strategy.

Keywords: cyberspace, cyber security, society, vision, goals, scope, method, strategy, action plan.

Introduction

The cyberspace today becomes the unavoidable part of today's society in its virtual dimension. The nations and international community invest significant efforts to assure certain terms and responsibilities in this virtual dimension of the society. These terms and responsibilities are comparable to what we have in the physical dimensions of our society. As a result of this approach many national cyber security strategies, including European Union (EU) and North Atlantic Treaty Organization (NATO) strategies, in a very short time have become highly positioned on today's political agendas. The questions about the responsible institutions to address in the strategy, guiding principles to follow, and the way of implementing the strategy, still remains very differently approached within different nations. At the same time, the huge number of countries shares the same societal values and expectations, and many of them even share the membership or partnership status within EU and NATO.

Within the proposed approach in this paper, all these challenges in the creation of national cyber security strategies are taken into account, focusing primarily on harmonising very heterogeneous content of a cyber security strategy with different national and international requirements and expectations. The goal of this paper is to define a more consistent approach to the process of the development of national cyber security strategies. The proposed approach is focusing primarily on the definition of scope of a cyber security strategy and the method for harmonising and adjusting very heterogeneous content of a strategy with the variety of national and international requirements and expectations.

The key research question is whether the proposed approach results in a more consistent national cyber security strategy that covers all the necessary national requirements and expectations, one that is easier to harmonise with different international requirements and expectations. In order to verify the proposed approach, the article provides a brief overview of the results achieved in the case of the development process of Croatia's National Cyber Security Strategy following the proposed method.

The Cyberspace and the Need for a Cyber Security Strategy Development

For the purpose of this article, the cyberspace is defined as the global virtual environment of mutually interconnected public and private information systems. Different types of information are generated, stored, and transmitted within cyberspace, including certain specific types of information that are dominant considering information security requirements in general, as well as different national and international laws and regulations.[1]

Unlike simple electronic services offered in the beginning of the Internet and then spreading throughout the world, today's cyberspace has completely changed people's private and professional life, as well as it has changed the infrastructure of most business sectors including the way of doing business in many cases. Change from dial-up technology to broadband connections that are always on-line, from the traditional plain old telephone services (POTS) to today's triple play household connections with VoIP telephony (Voice over Internet Protocol), IP television, and Internet connection, from fixed telecommunications to mobile telecommunications, is the change that happened during the last 20 years of the rapid technology development. IP based services have become the necessity in the contemporary society, either as the widespread web content, as the variety of social networking applications, or as the possibility of cloud data storage and cloud computing services. All these technologies and different types of services hugely support the actual globalization process in the world and, at the same time, they have become the necessity for the Government sec-

tor, Business sectors and Citizens (GBC) in the nations around the world. In that way the rapid technology development has introduced huge changes in the business processes and the way of citizens' living, affecting very deeply not only the technology as one of the key factors of all security policies, but also the processes and people as other two key factors.

Such new virtual dimension of our living has introduced some specific threats and attack possibilities, but it has also opened up a new dimension for different kind of traditional threats, such as the general fraud and theft threats. Many GBC users and infrastructures each day become more and more exposed to the variety of cyber threats. It is due to many factors that characterise the cyberspace today. Some of the main factors are:

- The increasing computing technology dependency;
- Lack of security and privacy awareness among computer users;
- Wide availability of software tools that can be used for computer attacks;
- Variety of new types of threat actors in cyberspace;
- Non-existence of state borders in cyber attacks and asymmetric nature of cyber attacks; and
- Insufficient preparedness and coordination of governments and international institutions for this virtual dimension of the society – the cyberspace.

Many nations and international organizations have invested considerable efforts during the recent years to assure certain terms and responsibilities in this virtual dimension of the society. These terms and responsibilities are comparable to what we have in the physical dimensions of our society. As the result of this, many initiatives to develop national cyber security strategies, as well as EU and NATO strategies, in a very short time become highly positioned on today's political agendas.[2,3]

In spite of all these efforts, the questions about the responsible institutions to address in the strategy, guiding principles to follow, and the way of implementing the strategy, still remain approached in a rather different manner within different nations. Most countries share the same societal values and expectations, and some of them share the membership or partnership status in EU and NATO. These different national approaches to cyber security therefore may represent certain kind of obstacle to further societal development due to the globalised market economy, and common standards that need to be established in many business and societal sectors of different nations.

The actual proposal of EU Network and Information Security (NIS) Directive [4] covers much more areas (e.g. critical infrastructure protection, CERT/CSIRT hierarchy, information sharing, etc.) and not only the traditional telecommunication sector issues. It is an example of the complexity that comes out from the cyberspace. This

complexity needs to be harmonised on the EU level, assuming the same or at least similar level of cyber security standards in all EU member states. One of the ways to achieve the comparable level of standards in this virtual dimension of society in different nations is through the vision of cyber security strategy that has the same underlining thoughts of the vision – the cyberspace as the virtual dimension of the society.

The Proposed Method for the Development of Cyber Security Strategies

The viewpoint that considers cyberspace as the virtual dimension of the society introduces the huge, complex, heterogeneous and mutually interrelated content of a cyber security strategy. The requirements for that content are drawn either from government or from business sectors/subsectors, either nationally or internationally. A comprehensive coordination and management system needs to be established and has to rely on responsible organizations from different societal sectors, regulated by different national and international laws and regulations. The strategy drafting process has to be organized with a number of diverse institutions that are stakeholders in certain parts of this huge field of cyber security. Moreover, the final proposal of a national strategy has to be communicated and harmonised on the widest level of the society.

The development of a consistent strategy document with such complex requirements should be based on a method that will assure consistency of the results obtained through the various development phases and diverse stakeholders that need to participate in the strategy development process. Using such method for a strategy development should also allow for much easier way to periodically update or revise the strategy. Moreover, using the similar approach in different national environments allows much easier harmonisation of the security standards in the virtual dimension of the society on a wider scale, e.g. within the international organizations consisted of different member states such as NATO or EU.

Following the introductory discussion, a cyber security strategy is considered as a way to identify key societal sectors and subsectors, to assess specifics of these sectors, to identify organisational prerequisites, to assess the threat environment in the area of interest, and to establish a comprehensive coordination and management process. The guidelines for the definition of the scope of a cyber security strategy are therefore proposed in the first subchapter. These guidelines are used for the very important part of the process of drafting a cyber security strategy. It is an assessment of the very specific and localised cyberspace characteristics. The assessment process is structured into five areas recognized by the proposed method as the most important ones. This allows more consistent approach to the very huge and diverse content that need to be elaborated within a cyber security strategy. Different security requirements come from different sectoral sources, as well as both from the national and interna-

tional environment. This leads to very complex cross sectoral organisational requirements in order to achieve the comprehensive and efficient coordination and management process.

The basic strategy elements, introduced in the second subchapter as part of the proposed method, are used for comprehensive and consistent approach to elaboration of specific and localised selection of key cyber security areas and interrelations for a strategy. The third subchapter introduces cyber security areas that are viewed as the pillars of a strategy, whereas interrelations of these areas are cross sectoral and functional areas that have to be efficiently coordinated in order to have complementary approach that results in cross sectoral synergy (e.g. security awareness initiatives). The implementation phase of each strategy requires certain kind of action plan. A cyber security strategy is sensitive to inefficient implementation due to its high complexity that comes out from the deep interdependencies among today's technology and global society. In the proposed approach in the fourth subchapter, the implementation phase of a strategy is viewed as an integral part of the strategy drafting process. The measures in an action plan in that way are direct elaboration of all specific goals that represent specific localised cyber security areas and selected interrelations of these areas.

The method for the development of a cyber security strategy, proposed in this article, is further elaborated in the following subchapters.

The Scope of a Cyber Security Strategy

A cyber security strategy is one of the foundations for building the virtual dimension of the society, together with other related strategies focusing on the issues such as: digital society, digital economy, access and connectivity, etc.[5] Most of the national cyber security strategies, especially the ones developed after 2010, are initiated based on the viewpoint that consider the cyberspace as the virtual dimension of the society.[6,7,8] A vision elaborated on the base of this viewpoint implies the development of certain capabilities and mutual coordination of all the societal sectors in order to achieve the protection of core values of liberty, fairness, transparency and the efficient rule of law within the virtual dimension of today's society.

A cyber security strategy needs to elaborate the way to achieve the selected vision within that part of the scope that refers to the security issues of the virtual dimension of society. Following the reasoning presented in the previous chapters of the article, the more comprehensive analysis has been done, resulting in the following guidelines for the definition of the scope of a cyber security strategy. The five key areas important for the scope definition have been identified as follows:

- Identification of societal sectors/subsectors;

- Assessment of sectoral specifics;
- Identification of organisational prerequisites;
- Assessment of the threat environment; and
- Establishment of comprehensive coordination and management process.

These five areas are briefly discussed in the following subchapters.

Identification of Societal Sectors/Subsectors

Previously defined initial viewpoint of the cyberspace as the virtual dimension of the society serves for the localised strategy vision definition. It implies that a cyber security strategy has to cover all of the three main sectors of the society: government, business and citizens. Besides these sectors, the inclusion and careful analyses of the potential role of academic sector has to be done. Very high complexity of the technology that is used within the cyberspace, as well as the complexity of cyber attacks, combined with the globalisation and social behaviour issues, inevitably demands the involvement of academic sector.

The particularities in government sector are usually related with the functional areas such as cybercrime, cyberterrorism, or cyber defence. The taxonomy of cyber terminology unfortunately is not standardised yet, so in many cases the terms “cyber security” and “cyber defence” are used interchangeably. Within the proposed approach in this paper, the term “cyber defence” is used as a functional subarea of cyber security, and is treated as the part of a military doctrine, which should rely on the resources and practises established by the respective national cyber security strategy. Alternatively, such functional subarea as cyber defence can be defined with a separate substrategy.

As far as both the government and business sectors are concerned, further particularities come mainly from the field of communication and information infrastructure that is used (public telecommunications, government infrastructure, critical information infrastructure, etc.), as well as from the specific groups of electronic services offered to the citizens (e-Government, e-Banking, e-Commerce, etc.).

Assessment of Sectoral Specifics

The most important specifics of the societal sectors come from the sectoral laws and regulations. Sectoral laws and regulations normally define responsible institutions (e.g. National Regulatory Authority – NRA), business terms and responsibilities, including the binding security standards, and the definition of sensitive types of information. Besides that, sectoral laws and regulations in many cases are closely interrelated with certain international regulatory framework such as Basel standards for

banking sector, or some EU directives that are obligatory for certain sectors of EU member states.[9]

Certain national initiatives among different sectors represent the necessity today (e.g. information sharing, security education and awareness) but these initiatives have to be carefully planned due to the possible limitations based on the rules already introduced in some of the sectors. Figure 1 illustrates the complexity of the cyberspace regulation framework, based on the previously introduced definition of the cyberspace.[1,9]

Identification of Organisational Prerequisites

A cyber security strategy covers a vast area of the society, so the organisational prerequisites are highly complex. These prerequisites are implicitly contained within some parts of cyberspace regulation framework and can be derived from the Figure 1.

The main organisational emphasis in a cyber security strategy should be on the policy planning bodies, not only for the purpose of strategy drafting process, but also in order to harmonise particular and specific sectoral policies with the national one. Equally important is the harmonisation of the national policy with different international requirements that can come through many sources (e.g. NATO, EU, international business sectors standards). This is the area mainly covered by the responsibilities of the bodies such as National Security Authorities (NSA) and National Regulatory Authorities (NRA), as well as different coordination bodies in the areas such as critical infrastructure protection, crisis management, etc.

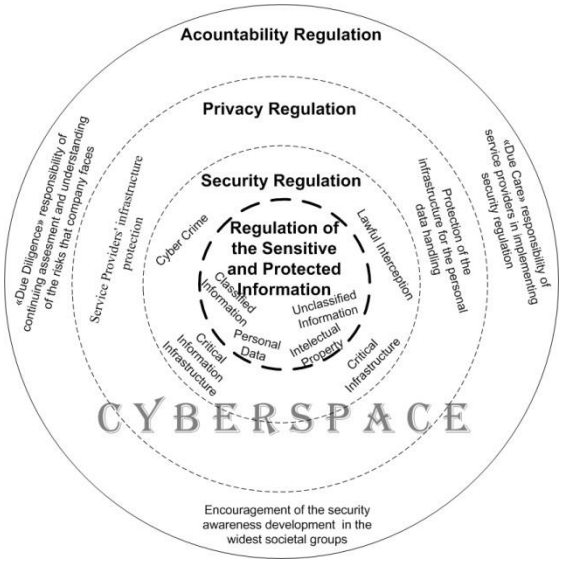

Figure 1: The Cyberspace Regulation Framework.[1,9]

National regulatory authorities (NRA) are normally established within the business sectors such as telecommunication sector or banking sector. Besides that, NRA bodies are typical authorities that regulate functional areas related to some or all of the societal sectors such as the NRA body responsible for personal data protection. Coordination bodies in the critical infrastructure protection area normally are divided between the main coordination body and sectoral coordination bodies based on the relevant national regulation that establishes national critical infrastructure sectors. Other coordination bodies in the area of crisis management are closely connected with the area of critical infrastructure protection and the cyber security incident coordination bodies.

National body responsible for National CERT/CSIRT functionality (Computer Security Incident Response Team), together with other similar bodies established throughout all of the societal sectors (sometimes called national CERT/CSIRT hierarchy), represent one of the main points for the successful implementation of a cyber security strategy. Other closely related and important technical bodies are Certificate Authorities (CA) that are generally responsible for the issuance of digital certificates, among others based on the relevant digital signature legislation. This field is further related with the national/international standardization authorities and other delegated authorities for accreditation and certification processes.

Other necessary bodies that should be identified for the purpose of coordination and management come from the previously mentioned functional areas such as cybercrime, cyberterrorism, or cyber defence. These functional areas may be coordinated separately from the national cyber security strategy because of the particularities and limitations that stem from such functional areas (e.g. cyber espionage). Even in that case, the responsible bodies for such functional areas should be clearly defined in order to allow two-way communication with other responsible bodies defined within a national cyber security strategy framework and to allow that such functional areas with separately developed policy (sub-strategy) can rely on all of the resources and practises established by the respective national cyber security strategy.

Assessment of the Threat Environment

Shared cyberspace environment with no borders implies that the cyber threats are shared. However, the cyber threats are not uniformly dispersed throughout the cyberspace. For the purpose of the scope definition for the development of a cyber security strategy, certain high-level assessment of the typical threat distribution in the area of interest should be done.

Certain considerations should be taken into account such as the specifics of the national communication and information infrastructure, the state of development of tel-

ecommunication sector and other infrastructure, the state of availability and development of electronic services in typical sectors like banking sector or government sector, etc. The geopolitical situation is also one of the main concerns because of the high probability of creating different types of politically caused cyber threat actors.

Generally, national and regional specifics lead to a different exposure to certain risks in different areas. More developed electronic services and infrastructure tend to be more prone to the cyber attacks such as DDOS (Distributed Denial of Service). On the other hand, even in the case of less developed and not very advanced technical infrastructure, or in the case of air-gap Internet isolated information systems, valuable or secret information could be more prone to sophisticated APT (Advanced Persistent Threat) cyber attacks.

The relevant national early warning system [10] with the established exchange of information on cyber security incidents among different global/regional/national players in CERT/CSIRT field, together with the organizations and companies specialized in cyber security, could be of great value for the high-level national or regional trend analysis in this field.

Establishment of a Comprehensive Coordination and Management Process

A comprehensive coordination and management process has to comprise the defined scope of strategy that comes out from the established vision. In order to deal with the complexity of the cyberspace, a cyber security strategy planning process should be separated into strategic, tactical, and operational and technical levels, according to Figure 2. In this way, it will be possible to differentiate between the national level of strategies/policies and tactical levels of sectoral policies, taking into account all of the necessary international requirements duly harmonised with the proper national or sectoral policy levels.

Specifically for cyberspace, it is of great importance to differentiate between the societal sector issues that are mainly related to the strategy coordination and management processes (Strategic and Tactical levels from Figure 2) and technical and operational issues related with the proper enforcement of a strategy (Operational and Technical level from Figure 2). To be able to solve properly these operational and technical problems, they need to be appropriately supported on the higher tactical and strategic levels. In this way, an institutional framework for coordination and management has to consist of the properly adjusted purview of the relevant authorities mutually coordinated according to the levels of Figure 2. Such coordination has to be adequately supported vertically by relevant national authorities, and horizontally among necessary societal sectors and relevant sectoral authorities.

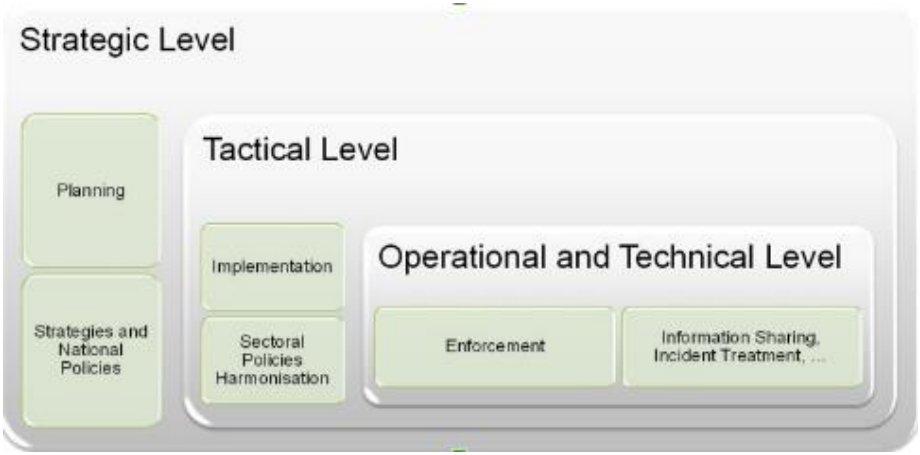

Figure 2: The Levels of a Strategy Planning Process.

The Basic Strategy Elements

The starting point for the elaboration of a localised strategy vision and the leading underlining thoughts of the vision is the understanding of cyberspace as the virtual dimension of the society. The localised vision of a strategy has to be properly elaborated from that starting point in order to serve very specific and localised environment. This means that the basic strategy elements have to be selected using the results of the assessment according to the proposed guidelines for the development of a cyber security strategy scope that are applied to a targeted national environment.

The recommended starting point of "the cyberspace as the virtual dimension of the society" supports localised elaborations of a strategy vision in two important directions. Firstly, from a national viewpoint, it allows comprehensive cross sectoral approach covering all three security policy key factors: people, processes and technology. Secondly, from the international viewpoint, it helps in harmonising localised visions in different national strategies, and such harmonisation is becoming the necessity in today's globalized world.

The proposed approach further elaborates a localised strategy vision with the selection of the basic strategy elements. The basic strategy elements are: general strategy goals, main principles, societal sectors, and the way of stakeholders' cooperation. The examples of general strategy goals are: "Raising societal security awareness …," "Comprehensive approach to international cooperation …," "Enforcement of the activities and measures with the goal to improve security, resilience and reliability of cyberspace …," etc. These general strategy goals have to be selected based on the assessment of the state of virtual dimension of the society in the area of interest (e.g. na-

tional environment). This assessment is done following the guidelines for the development of a cyber security strategy scope proposed in this article.

The general strategy goals have to be supported by the selected and defined societal sectors that the strategy refers to (e.g. GBC sectors, academic sector), by the main selected strategy principles (e.g. "proactiveness," "subsidiarity," "proportionality," "integration," etc.), and by the selected way of stakeholders' cooperation (e.g. public sector coordination, inter-sectoral cooperation, international cooperation, etc.). These basic strategy elements are illustrated in the upper left corner of Figure 3 that represents the elaborated and localised strategy vision derived from the initial underlining thoughts that the cyber space represents the virtual dimension of the society.

Cyber Security Areas and Interrelations of the Areas

The next step of the proposed method is the selection of the main recognized cyber security areas [11] based on the assessment that is done following the guidelines for the development of a cyber security strategy scope proposed in this article. These cyber security areas have to be selected based on the assessment of the state of the virtual dimension of the society in the area of interest (e.g. national environment).

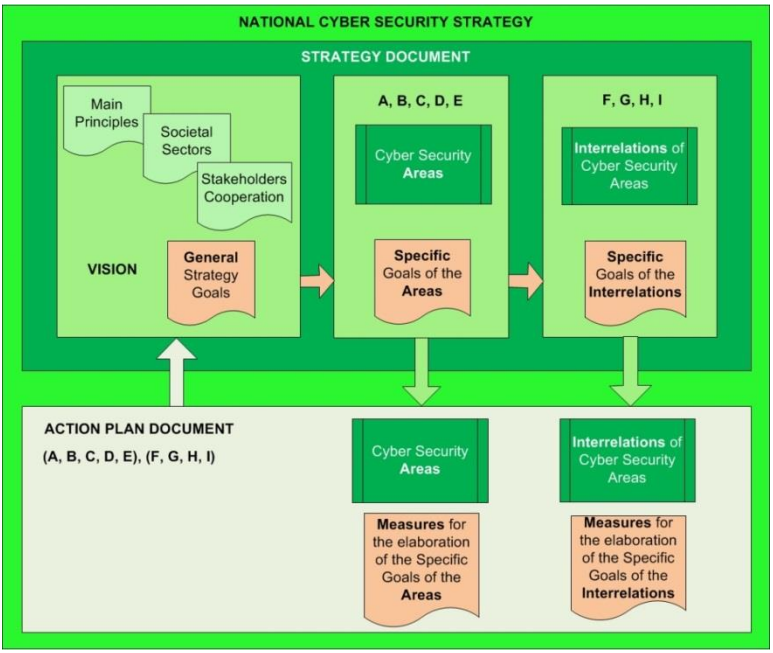

Figure 3: The Method for the Elaboration of a Cyber Security Strategy and Associated Action Plan.

According to Figure 3, for each selected cyber security area marked as A, B, C, D, E on Figure 3 (e.g. "Financial e-Services"), specific goals of that area have to be defined based on the assessment of the area of interest (e.g. national environment). These specific goals of the area have to support general strategy goals and have to refer to all relevant societal sectors, sticking thereby to the main selected principles (Figure 3).

Interrelations among selected cyber security areas marked as E, F, G, H on Figure 3, represent functional requirements (e.g. "International Cooperation") that are spread across all or the most of selected cyber security areas.[11] According to the Figure 3, for each selected interrelation (e.g. "Protection of sensitive information"), specific goals of that interrelations have to be defined based on the assessment of the area of interest (e.g. national environment). These specific goals of the interrelations have to support specific goals of all cyber security areas that the relevant interrelation interconnects, and they have to refer to all relevant societal sectors, sticking thereby to the main principles (Figure 3).

Figure 3 illustrates the explained reasoning and shows the way in which the consistency of initial vision and general goals is assured throughout of this very complex strategy development process that consists of a number of stakeholders and players.

The Correlation between a Strategy and its Implementation Action Plan

A strategy has to be followed by the relevant action plan that contains the measures elaborated for the implementation of all of the specific goals defined in the strategy document. This is shown in the lower part of the Figure 3. In this method, it is proposed that each of the specific goals, both for the selected cyber security areas and for the selected interrelations of the areas, is elaborated with one or more measures within the action plan document. In this way, these measures are fully consistent with the strategy vision and all general strategy goals, because all of the specific goals of the areas and interrelations support the selected general strategy goals (Figure 3). This assures the consistency between both documents – the strategy document and the action plan document that serves for the implementation of the strategy.

Croatia's National Cyber Security Strategy Drafting Process

Croatia's National Cyber Security Strategy drafting process started in April 2014 based on the Croatian Government Decision to form an interdepartmental committee for drafting the National Cyber Security Strategy. The development process was done under the auspices of the Office of the National Security Council as the leading institution.

The Interdepartmental Committee for the Croatian National Cyber Security Strategy drafting process consisted of more than 20 different institutions, whereas more than 30 institutions where actively involved in the activities of nine working groups covering different strategy development elements (five selected cyber security areas and four selected interrelations of these areas). Croatia's Cyber Security Strategy proposal was published for the purpose of public discussion in April 2015 [12] and it was adopted by the Croatian Government in October 2015.[13]

The Scope of the National Cyber Security Strategy

The Scope of the National Cyber Security Strategy was elaborated based on the guidelines for the development of a cyber security strategy scope proposed in this article and using the experience acquired mainly from the framework of implementation of Croatian National Information Security Programme adopted in March 2005.[14] The National Information Security Programme covered mainly traditional information security policy of the government sector. Besides covering all the necessary government security policy elements, it introduced very advanced approach that covers both the classified and unclassified information, as well as the establishment of National CERT functionality within the academic sector, but under the auspices of the Office of the National Security Council in the role of Croatian National Security Authority (NSA) (Figure 4).

Other inputs used for the scope definition of the Croatian National Cyber Security Strategy came from several associated activities. One of these associated activities was the analysis of the state of play and the possible threats to the public telecommunication system, done in 2009 and 2010 by the Office of the National Security Council together with a few other Croatian ministries and agencies. Furthermore, a National Early Incident Detecting System (SRU@HR),[10] developed by the Croatian National CERT in 2011, was also a valuable source for the assessment of threat trends, types, and relevant risk. Another valuable source of experience for the scope definition was the process of development of the "Ordinance on the Method and the Terms for the Implementation of the Measures for the Protection of Security and Integrity of the Networks and Services."[15] This ordinance was developed in 2012 by Croatian telecommunication NRA body (HAKOM), together with the ministry responsible for telecommunication sector, Croatian National CERT, and the Office of the National Security Council as Croatian NSA body.

The Basic Elements for the Development of Croatian National Cyber Security Strategy

Based on the proposed method for the development of a cyber security strategy, the process of drafting Croatian National Cyber Security Strategy and the selected basic

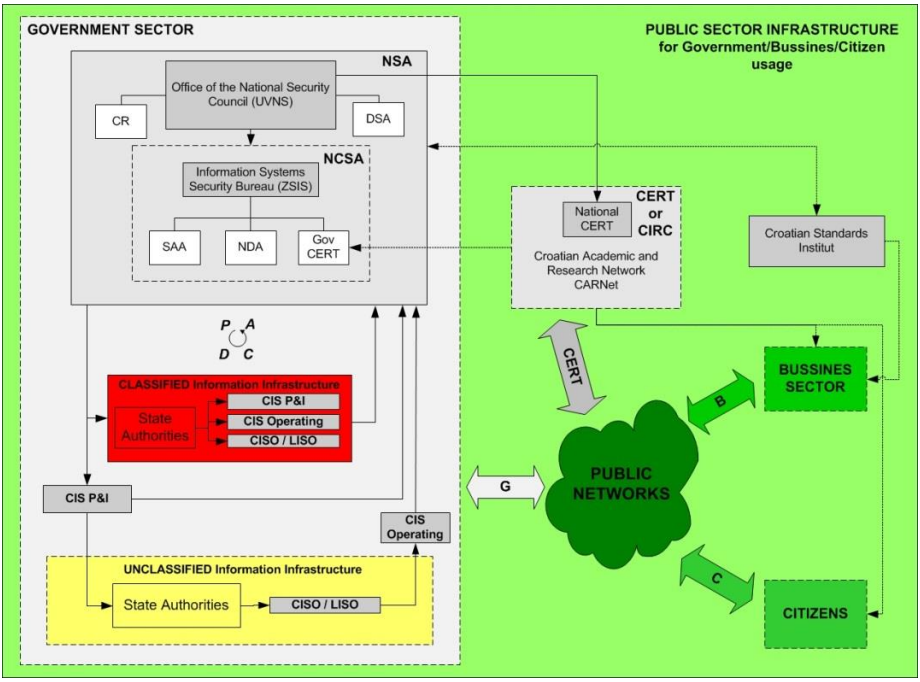

Figure 4: Croatian National Information Security Programme Adopted in 2005.

elements of the method are shown in Figure 5. It can be seen that the green area in the Figure 5 actually represents further elaborated green area from the Figure 4. This public sector infrastructure from the previous National Information Security Programme from 2005,[14] in the National Cyber Security Strategy from 2015 [13] is further elaborated in a much more comprehensive way following the initially introduced viewpoint of cyberspace as the virtual dimension of society (Figure 5).

Besides the assurance of the consistency of the vision, goals and measures, as it is explained in the previous chapter, the proposed method opens the possibility of modular approach to the development of this structured strategy content. In such way, the five selected cyber security areas and the four selected interrelations of these areas were separately developed by nine working groups that worked in parallel under the coordination of the Office of the National Security Council. The consistency of the results of all these working groups is assured by using the proposed method explained in the Figure 3.

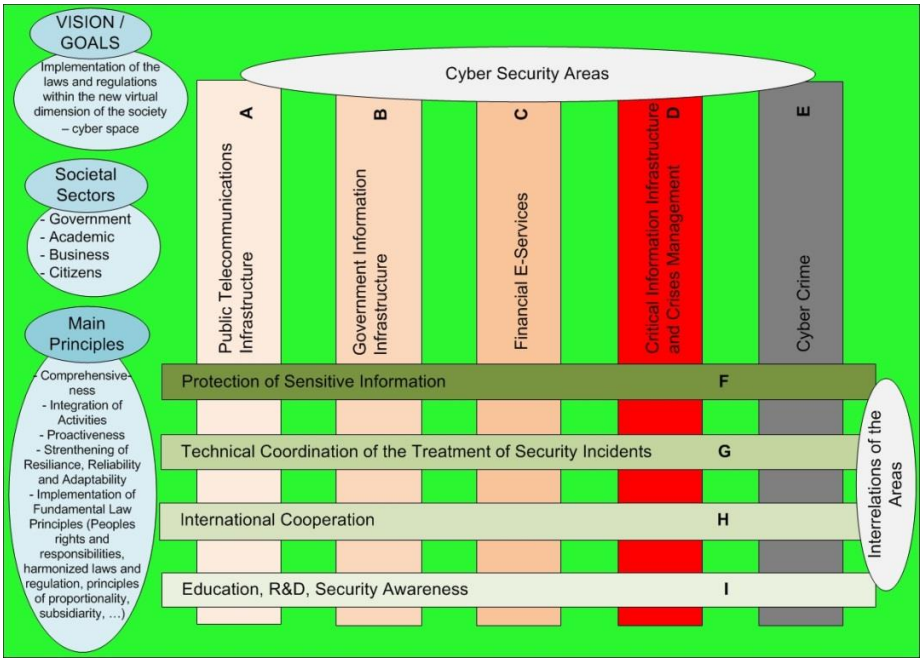

Figure 5: The Illustration of the Main Strategy Elements Selected for the Elaboration of the Croatian National Cyber Security Strategy.

The Correlation between the Strategy and the Action Plan Documents

The vision defined in the strategy document is supported by eight general strategy goals. These eight general strategy goals were further elaborated with 18 specific goals of the five selected cyber security areas. These 18 specific goals of the five selected cyber security areas were further supported by 17 specific goals of the four selected interrelations of the cyber security areas. Finally, all these 35 specific goals of the areas and interrelations were further elaborated with 77 measures within the Action Plan document.

The mentioned consistency of the proposed method assures that these 77 measures are in line with general strategy goals and the initial strategy vision. Thereby, these measures in the Action Plan document support the assessed cyberspace situation in Croatia based on the reasoning shown in the previous chapter, and the discussion of the localised strategy development process shown in this chapter.

The distribution of the elaborated measures across the selected cyber security areas and interrelations of these areas confirmed the expectations based on the scope as-

sessment. The mostly addressed areas in the strategy proposal (Table 1) were expectedly the area of "Education, Research and Development, and Security Awareness" ("I"), "Critical Information Infrastructure and Crises Management" ("D"), and "Government Information Infrastructure" ("B"). The area of "Education, Research and Development, and Security Awareness" ("I") consists of horizontally aligned all of the previously separated sectoral activities in this area. The reason for such approach is the necessity of coordination of all these activities on the national level in order to manage them properly among different sectors where they have to be applied with much more complementary approach. The area of "Critical Information Infrastructure and Crises Management" ("D") is relatively new area in Croatia consolidated by the law enacted in 2012. This area needs to be further elaborated and improved, especially in the area of critical information infrastructure and their interdependencies. The area of "Government Information Infrastructure" ("B") is focused on a lot of measures mainly because of the new activities based on the new Law on Government Information Infrastructure adopted in 2014, and the newly introduced very complex e-Citizen information services project.

Table 1: Croatian National Cyber Security Strategy [13] and the resulting number of specific goals and measures spread across the selected cyber security areas (A, B, C, D, E) and interrelations of the areas (F, G, H, I).

Areas and Interrelations	***Cyber Security Areas***					***Interrelations of the areas***			
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**
Specific Goals (35)	3	3	2	5	5	5	3	6	3
Measures (77)	3	8	4	13	5	6	5	6	27

On the other hand, the least number of measures are planned in the area of "Public Telecommunications Infrastructure" ("A") and in the area of "Financial Services" ("C"). This is also something that can be easily comprehended following the National Cyber Security Strategy scope assessment. These two sectors in Croatia are highly developed considering the use of cyberspace, the sectoral organization, the used technology and the information services they offer today. The only problems assessed in these sectors have concerned the need to further improve the cooperation with other cyber sectors/areas. That is why the most of the measures for these two sectors that are proposed by the strategy, are actually the measures in the segments of interrelations of these cyber security areas and not directly within the respective two cyber security areas (Figure 5).

Conclusion

A method for the development of a cyber security strategy is proposed in this paper. The reason for proposing this new approach for creating cyber security strategies is primarily the globalised and shared cyberspace, together with the necessity of international cooperation in this new, virtual dimension of the society. The approach proposed in this method takes into account various challenges in today's society, focusing primarily on harmonising very heterogeneous content of a cyber security strategy with different national and international requirements and expectations. The resulting method offers consistent approach to the process of the development of a national cyber security strategy. The strategy that is developed following this method is harmonised with all the necessary national needs and expectations, and at the same time, the resulting strategy has all the elements needed for efficient international cooperation—both at the national and sectoral levels—that need to be mutually harmonised.

The verification of the proposed method was done through the development process of Croatia's National Cyber Security Strategy. Besides the consistency and the flexibility for further harmonisation of the resulting strategy document, the method assured a very efficient framework for the cooperation of a huge number of different institutions – strategy stakeholders, that was necessary throughout the development process of the national cyber security strategy. Moreover, all of these stakeholders were efficiently managed using the proposed method in spite of the fact that most of them initially had rather different cyber security viewpoint and organizational maturity levels. The results of the verification process are described in the article together with the brief discussion of the achieved results. The verification process proves the achieved harmonisation with the necessary national requirements and expectations. At the same time, the resulting strategy structure is consistent and well-coordinated, and it offers flexible and coordinated way for international cooperation in any of the diverse cyber security contexts.

The key research question, whether the proposed approach results in a more consistent national cyber security strategy that covers all the necessary national requirements and expectations, and that is easier to harmonise with different international requirements, is in this way verified based on the process of developing Croatia's National Cyber Security Strategy.

Acknowledgement

This paper is based on the research implemented within the process initiated by the Croatian Government decision to form an interdepartmental committee for the drafting process of the National Cyber Security Strategy. The research was implemented under the auspices of the Office of the National Security Council [16] as the leading in-

stitution in the interdepartmental committee. The drafting process started in April 2014 and finished in October 2015 with the adoption of Croatia's National Cyber Security Strategy.[13]

Notes:

1 Aleksandar Klaic, *Knowledge Management Based Method for Modeling of Information Security Policies*, Doctoral Thesis (Zagreb: Faculty of Electrical Engineering and Computing, University of Zagreb, 2014), in Croatian, http://bib.irb.hr/lista-radova?autor=188115, accessed July 29, 2015.

2 ENISA, "National Cyber Security Strategies in the World," http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world, accessed on July 29, 2015.

3 NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), "Cyber Security Strategy Documents," https://ccdcoe.org/strategies-policies.html, accessed July 29, 2015.

4 European Commission, "The Directive on Security of Network and Information Systems (NIS Directive)," 16 March 2015, http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive, accessed on July 29, 2015.

5 European Commission, "Digital Agenda for Europe, A Europe 2020 Initiative," https://ec.europa.eu/digital-agenda/en, accessed July 29, 2015.

6 European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," February 2013, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf, accessed July 29, 2015.

7 "The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World," November 25, 2011, https://www.gov.uk/government/publications/cyber-security-strategy, accessed July 29, 2015.

8 "Austrian Cyber Security Strategy," 2013, https://www.bmi.gv.at/504/files/130415_strategie_cybersicherheit_en_web.pdf, accessed July 29, 2015.

9 Aleksandar Klaic and Anita Peresin, "The Impact of the National Information Security Regulation Framework on Cyber Security in Global Environment," in *International Scientific Conference on Corporate Security in Dynamic Global Environment – Challenges and Risks* (Ljubljana: Institute for Corporative Security Studies, 2012): 85-96.

10 Croatian National CERT, "Early Warning System on the Internet," www.cert.hr/en/sru_en, accessed July 29, 2015.

11 Alexander Klimburg, ed., *National Cyber Security Framework Manual* (Tallinn: NATO CCD COE Publications, December 2012), chapter 4, https://ccdcoe.org/multimedia/national-cyber-security-framework-manual.html, accessed July 29, 2015.

12 Office of the National Security Council, "Public discussion of the Croatian National Cyber Security Strategy Proposal," April 2015, https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=1072 (in Croatian), accessed on July 29, 2015.

13 "Government Decision on Adoption of National Cyber Security Strategy and the Action Plan for the implementation of the Strategy (in Croatian)," *Croatian Official Gazette*, nn 108, 2015, accessed on December 14, 2015.

[14] "Croatian National Information Security Programme" (in Croatian), March 2005, http://www.cert.hr/sites/default/files/CCERT-PUBDOC-2005-04-110.pdf, accessed July 29, 2015.

[15] "Ordinance on the Method and the Terms for the Implementation of the Measures for the Protection of Security and Integrity of the Networks and Services (in Croatian)," Croatian Official Gazette, numbers 109 (2012), 33 (2013), 126 (2013), http://narodne-novine.nn.hr/, accessed on July 29, 2015.

[16] Republic of Croatia, Office of the National Security Council, http://www.uvns.hr/en, accessed on December 14, 2015).

About the Author

Aleksandar KLAIC received the B.Sc. degree (1990) in Electrical Engineering and Computing, M.Sc. degree (1997) in Control Engineering, and a Ph.D. degree (2014) in Computer Science, all at the Faculty of Electrical Engineering and Computing, University of Zagreb. He works as Assistant Director responsible for information security at the Office of the National Security Council in Zagreb, Croatian National Security Authority (NSA). He has published more than 20 papers in journals and conference proceedings in the area of information security, control theory, and embedded systems. He is the founding member of the Croatian Association for the Robotics (HDR) and the member of international organizations IEEE and IACSIT.