Taylor & Francis
Taylor & Francis Group

Automatika

Journal for Control, Measurement, Electronics, Computing and Communications

ISSN: 0005-1144 (Print) 1848-3380 (Online) Journal homepage: http://www.tandfonline.com/loi/taut20

Cybersecurity and cyber defence: national level strategic approach

Darko Galinec, Darko Možnik & Boris Guberina

To cite this article: Darko Galinec, Darko Možnik & Boris Guberina (2017) Cybersecurity and cyber defence: national level strategic approach, Automatika, 58:3, 273-286, DOI: 10.1080/00051144.2017.1407022

To link to this article: https://doi.org/10.1080/00051144.2017.1407022

Published online: 25 Jan 2018.

AUTOMATIKA, 2017
VOL. 58, NO. 3, 273–286
https://doi.org/10.1080/00051144.2017.1407022

Taylor & Francis
Taylor & Francis Group

REGULAR PAPER

OPEN ACCESS Check for updates

Cybersecurity and cyber defence: national level strategic approach

Darko Galinec [a], Darko Možnik[b] and Boris Guberina[c]

[a]The Ministry of Defence of The Republic of Croatia, Zagreb, Croatia; [b]The Republic of Croatia Ministry of Defence, The Croatian Defence Academy, Zagreb, Croatia; [c]City of Zagreb – Emergency Management Office, Zagreb, Croatia

ABSTRACT

Cybersecurity encompasses a broad range of practices, tools and concepts related closely to those of information and operational technology (OT) security. Cybersecurity is distinctive in its inclusion of the offensive use of information technology to attack adversaries. Use of the term "cybersecurity" as a key challenge and a synonym for information security or IT security confuses customers and security practitioners, and obscures critical differences between these disciplines. Recommendation for security leaders is that they should use the term "cybersecurity" to designate only security practices related to the defensive actions involving or relying upon information technology and/or OT environments and systems. Within this paper, we are aiming to explain "cybersecurity" and describe the relationships among cybersecurity, information security, OT security, IT security, and other related disciplines and practices, e.g. cyber defence, related to their implementation aligned with the planned or existing cybersecurity strategy at the national level. In the case study given example of The National Cybersecurity Strategy of the Republic of Croatia and Action plan is presented and elaborated. The Strategy's primary objective is to recognize organizational problems in its implementation and broaden the understanding of the importance of this issue in the society.

ARTICLE HISTORY
Received 28 February 2017
Accepted 13 November 2017

KEYWORDS
Action plan, cyberattack; cybercrime; cyber defence; cyber operations; cybersecurity; national cybersecurity strategy; people-centric security

1. Introduction

Cybersecurity has been practiced in military circles for over a decade. In recent years, the term has appeared in a variety of contexts, many of which have little or no relationship to the original meaning of the term. Misuse of the term obscures the significance of the practices that make cybersecurity a superset of information security, operational technology (OT) security and IT security practices related to digital assets.

With the understanding of the specific environment, cyber defence analyses the different threats possible to the given environment. It then helps in devising and driving the strategies necessary to counter the malicious attacks or threats. A wide range of different activities is involved in cyber defence for protecting the concerned entity as well as for the rapid response to a threat landscape.

These could include reducing the appeal of the environment to the possible attackers, understanding the critical locations & sensitive information, enacting preventative controls to ensure attacks would be expensive, attack detection capability and reaction and response capabilities. Cyber defence also carries out technical analysis to identify the paths and areas the attackers could target [1].

2. Review of previous work

Military terminology has migrated into non-military contexts in the same fashion that military technology has migrated into civilian enterprises (e.g. the Advanced Research Projects Agency Network (ARPANET) becoming the Internet). Other terms, such as advanced persistent threat (APT; originally a euphemism for network attacks supported by the government of the People's Republic of China) [2], have endured similar transitions. In many cases, a migration of terminology is beneficial, as it develops better specificity in discussions of technology operations. However, the utility of a term is reduced when its distinctive meaning is eroded or destroyed as part of the migration to a new context.

2.1. Cybersecurity

Definition: Cybersecurity is the governance, development, management and use of information security, OT security, and IT security tools and techniques for achieving regulatory compliance, defending assets and compromising the assets of adversaries [2].

According to above-mentioned authors, cybersecurity

(1) is a superset of the practices embodied in IT security, information security, OT security and offensive security (see Figure 1);
(2) uses the tools and techniques of IT security, OT security and information security to minimize vulnerabilities, maintain system integrity, allow access only to approved users and defend assets;

CONTACT Darko Galinec darko.galinec@morh.hr

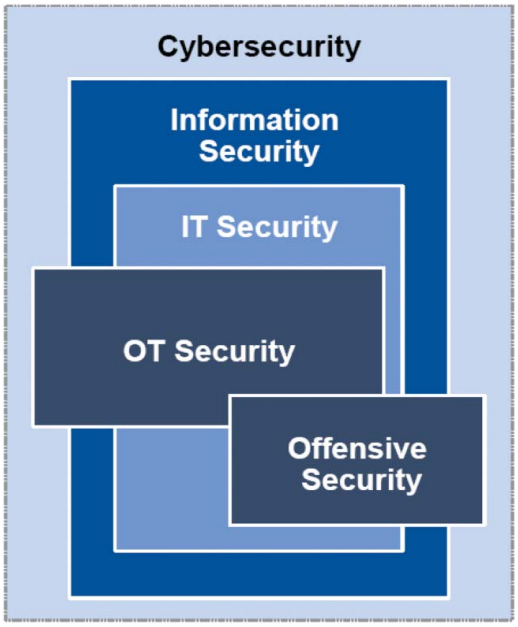

Figure 1. Components of cybersecurity.

(3) includes the development and use of offensive IT- or OT-based attacks against adversaries; and
(4) supports information assurance objectives within a digital context but does not extend to analogue media security (for example, paper documents).

But, in the same time, cybersecurity is not

(1) merely a synonym for information security, OT security or IT security and
(2) use of information security to defend an enterprise against crime.
(3) Cyberwarfare –although the definition of this term is still controversial, the consensus is that "cyberwarfare" refers to the use of cybersecurity capabilities in a warfare context. This is a complex area and should not be confused with physical attacks against infrastructure (e.g. destruction of property and machinery) and information warfare (e.g. applying psychological operations through propaganda and misinformation techniques).
(4) Cyberterrorism – in a similar fashion to cyberwarfare, "cyberterrorism" refers to the use of cybersecurity techniques as part of a terrorist campaign or activity.
(5) Cybercrime – cybercrime is merely an affected or pretentious term for criminal attacks using IT infrastructure. It is not related to cybersecurity.

Appropriate uses of "cybersecurity" [2] would be the following:

(1) In response to threat risk assessments, the department increased its cybersecurity investment to enable reductions in vulnerabilities and increased capabilities for counterattacks against identified attackers (integration of IT security and offensive capabilities in a single program).
(2) Integration of the IT and OT security programs within the cybersecurity team enables more holistic responses to threats (integration of IT and OT in a single program).
(3) The "hacktivist" organization Anonymous employs a variety of cybersecurity techniques to forward its agenda (use of offensive capabilities).

However, we could face with some inappropriate uses of "cybersecurity":

(1) In order to mitigate the theft of laptops, the store's cybersecurity plan calls for the use of wholedrive encryption. (This describes a basic IT security action.)
(2) The cybersecurity policy mandates the use of complex passwords for all CAM systems on the factory floor. (This describes a basic OT security requirement.)

2.2. Cyber defence

There are no common definitions for Cyber terms – they are understood to mean different things by different nations/organizations, despite prevalence in mainstream media and in national and international organizational statements [3].

However, [1] gives definition and further explanation of term cyber defence as follows: Cyber defence is a computer network defence mechanism which includes response to actions and critical infrastructure protection and information assurance for organizations, government entities and other possible networks.

Cyber defence focuses on preventing, detecting and providing timely responses to attacks or threats so that no infrastructure or information is tampered with. With the growth in volume as well as complexity of cyberattacks, cyber defence is essential for most entities in order to protect sensitive information as well as to safeguard assets.

Cyber defence provides the much-needed assurance to run the processes and activities, free from worries about threats. It helps in enhancing the security strategy utilizations and resources in the most effective fashion. Cyber defence also helps in improving the effectiveness of the security resources and security expenses, especially in critical locations.

By the recognition of the need to accelerate detection and response to malicious network actors, the United States (US) Department of Defense (DoD) has defined a new concept, Active Cyber Defence (ACD) as DoD's synchronized, real-time capability to discover, detect, analyse, and mitigate threats and vulnerabilities [4].

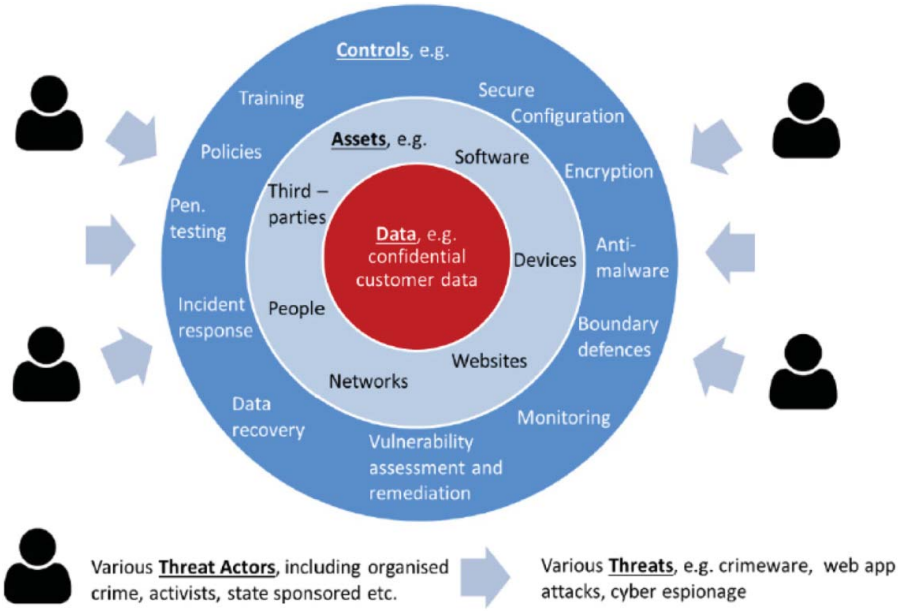

Figure 2. Cybersecurity key components and relationships.

2.3. People-centric security

People-centric security (PCS) is a strategy that represents an alternative to conventional information security practice. PCS aims to strike a balance between risk reduction and employee agility. It is a strategic approach to information security that emphasizes individual accountability and trust and de-emphasizes restrictive, preventative security controls. The conventional control-centric approach to information security is increasingly untenable in rapidly evolving and ever more complex technology, business and risk environments.

Security leaders in organizations with the appropriate culture should investigate whether some or all of the concepts and principles of PCS are applicable to their security strategies. Such an investigation should indicate areas where a more people-centric approach will enable more cost-effective, trust-based security [5].

PCS is based on a set of key principles, and on the rights and related responsibilities of individuals. The premise of PCS is that employees have certain rights. However, these are linked to specific responsibilities. These rights and responsibilities are based on an understanding that, if an individual does not fulfil his or her responsibilities, or does not behave in a manner that respects the rights of his or her colleagues and the stakeholders of the enterprise, then that individual will be subject to sanction.

(1) This compact of rights and responsibilities creates a collective co-dependency among employees, exploiting existing social capital within the enterprise.
(2) PCS principles presume an emphasis on detective and reactive controls, and transparent preventative controls, over the use of intrusive preventative controls.
(3) PCS favours the maximization of a trust space within which individual autonomy and initiative is encouraged.
(4) PCS presupposes an open, trust-based corporate culture, and associated executive awareness and support.
(5) PCS principles presume that individuals have the appropriate knowledge to understand their rights, responsibilities and associated decisions.

On the other hand, PCS is not

(1) a replacement for common sense defence in depth security;
(2) a relaxation of security requirements or behavioural standards;
(3) identity management, nor is it specifically focused on the digital identity of individuals;
(4) aimed at all individuals, but rather at employees of the enterprise; and
(5) (just about) security awareness and training [3].

2.4. Methodology

Figure 2 [4] illustrates key components and relationships related to cyber security:

(1) Cyber security breaches target Data, in most cases confidential data, such as customer records or other valuable information
(2) Data are stored, processed and communicated on, by or to Assets, such as software, networks, devices (servers, workstations, smart phones, etc.), websites, people and third parties

(3) Threat Actors, such as organized crime gangs, activists and nation states will deploy Threats, usually targeted at or via Assets to access Data
(4) Controls which defend against Threats are mostly applied to Assets and occasionally directly to Data
(5) Some Controls such as encryption of mobile devices protect against specific Threats, such as loss or theft of mobile devices, whereas other Controls, such as software patching protect against multiple Threats, such as crimeware, web app attacks, cyber espionage, etc.
(6) Threats will aim to exploit weaknesses (or vulnerabilities) in Controls to access Data
(7) If the right Controls are applied to the right Assets and they are implemented effectively relative to the level of Threat then the organization will be able to defend itself against the Threat. If this is not the case then a Data breach will occur.

3. Cybersecurity strategy, cyber operations and security risk management

While the cost of defending cyber structures as well as the payoffs from successful attacks keeps rising, the cost of launching an attack simultaneously keeps decreasing [6].

By the standard military definition, "strategy" is the utilization of all of a nation's forces, through large-scale, long-range planning and development, to ensure security or victory. For traditional wars against traditional monolithic opponents, that approach worked.

However, for today's world of asymmetric warfare and rapidly changing threats, the medical definition of strategy from Merriam-Webster's dictionary is more appropriate for addressing cybersecurity: "an adaptation or complex of adaptations (as of behavior, metabolism or structure) that serves or appears to serve an important function in achieving evolutionary success".

The key to increasing cybersecurity is getting to lower levels of vulnerability. Although threat awareness is important, by reducing vulnerabilities, all attacks are made more difficult [7].

3.1. Cyber operations

Cyber operations consist of many functions spanning cyber management, cyberattack, cyber exploitation, and cyber defence, all including activities. In their nature those activities are proactive, defensive, and regenerative. Here we shall mention ACD as a subset of cyber defence which focuses on the integration and automation of many services and mechanisms to execute response actions in cyber-relevant time.

ACD is comprised of a set of logical functions to capture details from enterprise-level architecture to operational realization with the primary objective to become a living part of Ministry of Defences' cyber operations to help defend the nation from cyber-based adversaries

Among the many needs of war-fighter operations, there is the need to be secure, which includes the concepts of hardening, protecting, attacking, and defending among the war-fighter domains of land, sea, air, space, and cyber. Cyber is an integrating capability for the other domains, as well as a standalone domain that has its own unique needs for cyber defence [8].

Cyber defence includes three complementary categories: "proactive", "active" and "regenerative". "Proactive" activities harden the cyber environment and maintain peak efficiency for cyber infrastructure and mission functions. "Active" activities stop or limit the damage of adversary cyber activity in cyber-relevant time. "Reactive" activities restore effectiveness or efficiency after a successful cyberattack.

These categories form a continuum of cyber-security activities occurring continuously and simultaneously on networks, integrated by a common framework of automation that includes ACD as a subset of integrated cyber defence. The focus herein is on ACD [8].

Furthermore, cyber defence includes employing non-real-time big-data analytics to find trends in historical data repositories; likewise, cyber defence includes actuarial-like predictions of future events.

Attacks in the non-cyber domains require physical proximity and time to execute (e.g. a bomb must be close to a target; a bullet must physically hit its target).

Cyber is unique in the lack of need for physical proximity to execute an attack (that is, anyone with an Internet connection is a potential participant in this worldwide battle space) and in the vastly reduced time required to perpetrate an attack (for example, bits on a wire travel much more quickly than traditional troops or munitions).

ACD addresses this vastly reduced time necessary for a successful attack by integrating many solutions to provide response actions in cyber-relevant time. Cyber-relevant time is a purposely vague term that accommodates the needs of the battle space.

If the battle space is a Central Processing Unit (CPU) and Random Access Memory (RAM), and the combatants are software applications vying for control, the cyber-relevant time is nanoseconds to microseconds. If the battle space is between two computers of close physical proximity, cyber relevant time is milliseconds to seconds. For a battle space between two computers on opposite sides of the world communicating via satellite links, cyber-relevant time is seconds. With live operators and delays inherent in cognitive processing, key strokes, and mouse clicks, cyber relevant time is seconds to minutes.

The requirements for ACD increase as the adversary becomes smarter and quicker [8].

ACD monitoring activity may provide data feeds to these analytics, and the ACD sense-making activity may take influence from these analytics in the form of decision support algorithms. However, these historical and future analytics are outside the scope of real-time processing and, therefore, outside the scope of ACD.

3.2. Cybersecurity risk management

Cyber security breaches, such as those at Ashley Madison, the US Office of Personnel Management and JP Morgan Chase have demonstrated the real and present threat from cyber breaches. Director of the National Security Agency and head of the United States Cyber Command, Admiral Mike Rodgers has been moved to state that 'It's not about if you will be penetrated but when' [9].

In response, there is an urgent need for organizations to truly understand their cyber security status and where necessary take urgent remedial actions to rectify weaknesses. If there is not sufficient visibility of cyber security status, organizations will not be able to manage cyber security risks and they will almost certainly suffer a breach.

"Visibility of cyber security status" means having the complete picture, with measurements so that we can answer the following questions:

(1) What are our current measured levels of cyber security risk across the Enterprise from the multiple threats that we face?
(2) Are these cyber security risks tolerable?
(3) If not, what is our justified and prioritized plan for managing these risks down to tolerable levels?
(4) Who is responsible and by when?

The ability to measure cyber security status is fundamental; if we cannot measure then we cannot manage. Security incident and event management (SIEM) and data analytics solutions can provide valuable indications of actual or potential compromise on the network but these are partial views, indicators of our overall risk status but not measurements of our risk status.

Similarly, threat intelligence services can identify data losses and provide valuable indications of actual or impending attacks but again these are not measurements of our risk status. The same can be said individually about outputs from compliance management, vulnerability management, penetration testing and audits.

Only by pulling together all of the relevant indicators and partial views can we develop overall risk-based measurement and visibility of our cyber security status [9].

When confidence in our cybersecurity risk measurements exists it is possible to respond to events and make decisions quickly, e.g.

(1) Be able to identify risks that we are not prepared to tolerate and have a clear and prioritized risk-based action plan for the control improvements necessary to reduce these risks to an acceptable level
(2) To have a better understanding of the implications from threat intelligence or outputs from SIEM and data analytics allowing faster, better targeted responses
(3) To develop risk-based justifications for investment in cyber security solutions and services.

But with the very high level of threat and high rates of change in both the threat and control landscapes we need to be able to refresh our view of our cyber security status on an almost daily basis.

Cybersecurity risk management which previously might have been an annual process as part of planning and budgeting is now a critical real-time facilitator in the battle against cyber breaches [9].

Cyber security breaches occur when people, processes, technology or other components of the cyber security risk management system are missing, inadequate or fail in some way. So we need to understand all of the important components and how they interrelate.

This does not mean that your risk management system needs to hold details of (for example) every end point and the status of every vulnerability on the network because there are other tools which will do that but the risk management system does need to know that all end points on the network have been (and are being) identified and that critical vulnerabilities are being addressed quickly.

3.3. Cyber resiliency

Cybersecurity success is essentially the result of an effective risk management process. However, this process is being challenged by the inherent complexity of systems, developed with vulnerable components and protocols, and the crescent sophistication of attackers, now backed by well-resourced criminal organizations and nations.

With this scenario of uncertainties and high volume of events, it is essential the ability of cyber resiliency

Cyber resiliency is the ability of a system, organization, mission, or business process to anticipate, withstand, recover from, and adapt capabilities in the face

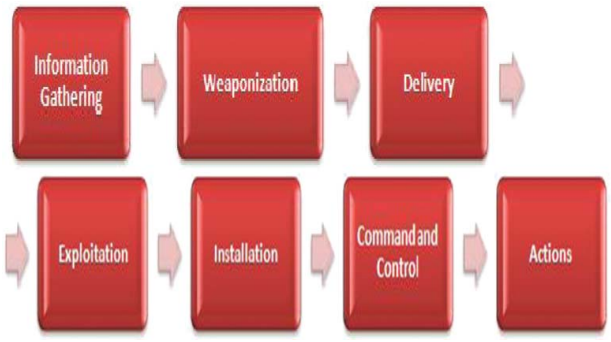

Figure 3. Intrusion Kill Chain.

of adversary conditions, stresses, or attacks on the cyber resources it needs to function.

3.4. Cyberattack model (intrusion Kill Chain)

The treatment of a cyberattack requires the use of an appropriate attack model. Using an attack model it is possible to recognize the current state of an attack and its possible future states. An attack model is a model of hypothesis which will be used to infer possible actions of attackers.

The Lockheed-Martin Intrusion Kill Chain (IKC) [10] model has been adopted as the central basis of our attack model. IKC is a model of seven stages that an attacker inescapably follows to plan and carry out an intrusion.

The IKC stages (see Figure 3) are presented as follows [11]:

(1) Information Gathering – Collecting target's information, such as used technologies and its potential vulnerabilities.
(2) Weaponization – developing malicious code to explore identified vulnerabilities, coupling the developed code with unsuspected deliverable payloads like pdfs, docs, and ppts.
(3) Delivery- Transferring the weaponized payload to the target environment.
(4) Exploitation – Use of vulnerabilities in order to execute the malicious code.
(5) Installation – Remote Access Trojan's (RAT) are generally installed which allows adversary to maintain its persistence in the targeted environment.

To defeat more sophisticated defence systems, attackers may require the execution of one or more IKCs to circumvent different defensive controls.

3.5. Cyber resiliency situational awareness

Cyber resiliency success is a result of timely and well-coordinated actions coming from an effective decision making process.

In a resilient system, defenders must be able to perceive the movement of attackers, understand the meaning of these movements, and take actions that will best counter these movements minimizing effects and allowing a rapid recovery of affected assets.

As in any conflict, the side that has information dominance has the greatest chance of victory. Achieving information dominance is about achieving SA (and denying it to the enemy). SA essentially answers the question of which data are as follows:

Command and control (C2). Adversary requires a communication channel to control its malware and continue their actions. Therefore, it needs to be connected to a C2 server.

Actions. it is the last phase of the kill chain in which adversary achieves its objectives by performing actions like data exfiltration. Defenders can be confident that adversary achieves this stage after passing through previous stages [11].

4. National cybersecurity strategy and action plan

The Internet has obviously become a relied-on communications infrastructure, much like the telephone system was a century ago. However, the evolution and technological underpinnings of the Internet are very different from that of telecommunications or any other infrastructure.

Thus, different approaches are required to ensure reliable and secure services in cyberspace than on the old telecom networks, and the development of public policy has to proceed very differently, as well. Gartner recommends that of national cybersecurity policy take a more realistic approach toward stimulating higher levels of security in cyberspace, rather than taking approaches that simply stimulate higher spending or higher visibility. Although there is definitely a role for government to play, driving higher levels of security in cyberspace through policy will be much more like trying to deal with global warming than like dealing with telephone, banking or automotive industry policies [7].

According to [7] a national cybersecurity strategy should leverage the strengths of the government to drive evolution of the standard security practices used by government agencies, businesses and citizens in their daily use of cyberspace.

The goals of such a strategy should be to define the current areas of shortcomings, apply leverage toward closing those gaps, assess progress and repeat.

A national cybersecurity strategy should not be aimed at having the government seek to control the level of security on the Internet or issue legislation to mandate solutions.

Cybersecurity is an inherently distributed problem that will continue to evolve at the speed of technology.

Thus, the cybersecurity strategy should focus on primarily eliminating or shielding vulnerabilities that enable attacks versus reporting attacks – like a hurricane preparedness strategy, which mandates redesigning structures or building higher levees versus the deployment of more water gauges.

4.1. Case study

The National Cyber Security Strategy [12] is a document with which the Republic of Croatia intends to start planning, in a systematic and comprehensive way, the most important activities for protecting all the users of modern electronic services, both in the public and economic sectors and among the general population.

4.1.1. Basic notions

The aim of the Strategy is to achieve a balanced and coordinated response of various institutions representing all the sectors of the society to the security threats in modern-day cyberspace. The Strategy recognizes the values that need to be protected, the competent institutions and measures for systematic implementation of such protection.

The Strategy is a statement of the cyber security stakeholders' determination to take measures in their respective areas of responsibility, cooperate with the other stakeholders and exchange the necessary information. It is a statement of their readiness to continue their own further development and adjustment, so that the Croatian cyberspace would be organized, available, open and safe to use.

The Strategy and Action plan for its implementation envisage the approach to cyberspace as the virtual dimension of the society. The goal of making the Strategy and implementing it by applying the measures elaborated in the Action plan is therefore consistent with the Cybersecurity Strategy of the European Union [13] and is directed towards achieving the maximum level of competence and coordination among all of our society's sectors, for an efficient implementation of law and protection of democratic values in the virtual dimension of today's society, that is, in cyberspace. Such a goal can only be achieved with a common, efficiently coordinated approach including a whole range of different institutions responsible for different sectors.

The reason for this lies in the fact that the very complex area of cyber security covers all the segments of the society and largely exceeds the technical area from which it once arose with the rapid development of the Internet and accompanying information and communication technologies.

The fundamental issue in cyber security is therefore the issue of organization, which is resolved in the Strategy through better and more effective connection of all the segments of the society, using as much as possible the existing bodies and their legal responsibilities.

The recognized objectives in different areas of cyber security should be achieved by applying the measures elaborated in the Action plan for each individual objective of the Strategy.

The description of the measures presented in the Action plan for the implementation of the Strategy shows that the Strategy will be implemented for the most part in the framework of the existing funds of the bodies competent for the activities in a particular measure and the bodies that will also be involved.

The added value of these existing funds and other resources is achieved through organizational measures for the harmonization and better coordination in various bodies' work on similar activities, a more efficient exchange of information and, generally, through the synergy of different institutions and society sectors that have so far not been sufficiently connected and coordinated when it comes to the activities related to cyberspace.

The intention of adopting the Strategy and Action plan and introducing a systematic and comprehensive approach to the area of cyber security is to achieve a number of objectives very important for the development of the entire society, in particular:

(1) Systematic approach in the application and development of the national legal framework to take into account the new, cyber dimension of the society.
(2) Implementing activities and measures to improve the security, resiliency and reliability of cyberspace;
(3) Setting up a more efficient mechanism for information sharing in order to ensure a higher level of general safety in cyberspace.
(4) Raising the awareness of security of all cyberspace users.
(5) Encouraging the development of harmonized education programmes.
(6) Encouraging research and development, particularly in the area of e-services.
(7) Systematic approach to international cooperation in the area of cyber security.

The methodology of approach chosen to define the contents of the Strategy was based on determining the general goals of the Strategy, society sectors covered by the Strategy, and basic principles of approach to the implementation of the Strategy.

Societal segments important for cyber security are divided into areas estimated to be of highest importance for Croatia at this level of development of the information society. The selected areas of cyber security are as follows:

(8) Electronic communication and information infrastructure and services, further divided into public telecommunications infrastructure, e-government infrastructure and electronic financial services.
(9) Critical communication and information infrastructure and cyber crisis management; Cybercrime.

Along with the areas of cyber security, the Strategy also recognizes the interrelations among the areas of cyber security, thus ensuring coordinated planning of all joint activities and resources in the mentioned cyber security areas. The following interrelations among the areas of cyber security have been selected:

(1) Data protection (groups of protected information, such as classified information, personal data, trade secret).
(2) Technical coordination in the treatment of computer security incidents.
(3) International cooperation.
(4) Education, research, development and raising the awareness of security in cyberspace.

The Strategy is based on the existing legislation and responsibilities, but it recognizes the need for certain laws to be revised through the implementation of the measures from the Action plan and harmonized with the recognized requirements of the society's virtual dimension, which has already become an integral part of both the private and professional lives and activities of all citizens and institutions.

The adoption of the Strategy cannot immediately solve all the problems that have occurred and accumulated throughout the past twenty years of rapid technological development and globalization of the society, the problems that are now present in every facet of our society.

The Strategy definitely represents the first step towards a systematic and lasting improvement of the current state in the area of cyber security and marks the beginning of introducing long-term and systematic care for all the future challenges in the society's virtual dimension, which is extremely important for the further development of the society.

4.1.2. Principles

Comprehensive nature of the approach to cyber security by covering cyberspace, infrastructure and users under the Croatian jurisdiction (citizenship, registration, domain, address);

Integration of activities and measures arising from different cyber security areas and their interconnection and supplementation in order to create a safer cyberspace;

Proactive approach through constant adjustment of activities and measures, and adequate periodic adaptation of the strategic framework they stem from;

Strengthening resilience, reliability and adjustability by applying universal criteria of confidentiality, integrity and availability of certain groups of information and recognized social values, in addition to complying with the appropriate obligations related to the protection of privacy, as well as confidentiality, integrity and availability for certain groups of information, including the implementation of appropriate certification and accreditation of different kinds of devices and systems, and also business processes in which such information is used;

Application of basic principles as basis of the organization of modern society in the area of cyberspace as the society's virtual dimension:

Application of law to protect human rights and liberties, especially privacy, ownership and all other essential characteristics of an organized contemporary society;

Developing a harmonized legal framework through continued improvement of all the segments of regulatory mechanisms of state and sector levels, and through harmonized initiatives of all the sectors of the society, that is, bodies and legal entities that are stakeholders in this Strategy;

Application of the principle of subsidiarity through a systematically elaborated transfer of power to make decisions and report on cyber security issues to the appropriate authority whose competences are closest to the matter being resolved in areas important for cyber security, from organization through coordination and cooperation to the technical issues of responding to computer threats to certain communication and information infrastructure;

Application of the principle of proportionality to make the level of protection increase and related costs in each area proportional to the related risks and abilities in limiting the threats causing them.

4.1.3. General goals of the strategy

Systematic approach in the application and enhancement of the national legal framework to take into account the new, cyber dimension of the society, keeping in mind the harmonization with international obligations and global cyber security trends;

Pursuing activities and measures to increase the security, resilience and reliability of cyberspace, which need to be applied in order to ensure the availability, integrity and confidentiality of the respective groups of information used in cyberspace, both by the providers of various electronic and infrastructure services and by the users, namely all legal entities and individuals whose information systems are connected to cyberspace;

Establishing a more efficient mechanism of information sharing necessary for ensuring a higher level of general security in cyberspace, whereby each stakeholder is required, especially concerning certain groups of information, to ensure the implementation of adequate and harmonized standards of data protection;

Raising security awareness of all cyberspace users with an approach that distinguishes between the particularities of the public and economic sectors, legal entities and individuals, and which includes the introduction of the necessary educational elements into regular and extracurricular school activities, along with organizing and implementing various activities aimed at making the broader public aware of certain current issues in this domain;

Stimulating the development of harmonized education programmes in schools and higher education institutions, through targeted and specialist courses, by connecting the academic, public and economic sectors;

Stimulating the development of e-services through building user confidence in e-services by defining the appropriate minimum security requirements;

Stimulating research and development in order to activate the potential and encourage harmonized efforts of the academic, economic and public sectors;

Systematic approach to international cooperation which makes possible an efficient transfer of knowledge and coordinated information sharing amongst the different competent national authorities, institutions and sectors of the society, with a view to recognizing and creating capabilities for successful participation in business activities in a global environment.

4.1.4. Sectors of the society and forms of cooperation of cybersecurity stakeholders

Defining the sectors of the society and their meaning for the purposes of this Strategy, as well as forms of cooperation of the cyber security stakeholders, also provided the definition of the scope of this Strategy.

For the purposes of the Strategy, sectors of the society and their definitions are as follows:

(1) Public sector with various competent authorities which are the stakeholders of the Strategy, other state authorities, bodies of local and regional self-government units, legal entities with public authorities and institutions representing in various ways the users of cyberspace and entities obliged to apply the measures arising from the Strategy.
(2) Academic sector in close cooperation with the state authorities which are the stakeholders of the Strategy, and other education institutions from the public and economic sectors representing in various ways the users of cyberspace and entities obliged to apply the measures arising from the Strategy.
(3) Economic sector in close cooperation with the competent state and regulatory bodies which are the stakeholders of the Strategy, especially legal entities subject to special regulations concerning critical infrastructures and defence, as well as all other legal entities and business entities representing in various ways the users of cyberspace and entities obliged to apply the measures arising from the Strategy, with all the particularities of those legal and business entities, with regard to their scope of work, number of employees and markets they cover.
(4) Citizens in general, representing the users of communication and information technologies and services. The state of security in cyberspace reflects on the citizens in various ways. It also refers to the citizens who do not use cyberspace actively, but their data are in cyberspace.

Forms of cooperation of cyber security stakeholders envisaged by the Strategy are as follows:

(1) Coordination within the public sector.
(2) National cooperation of the public, academic and economic sectors.
(3) Consultation with the interested public and informing the citizens.
(4) International cooperation of cyber security stakeholders.

All these forms of cooperation are carried out in a systematic and coordinated manner, in accordance with competences, capabilities and objectives, and according to the functionally elaborated cyber security areas defined in the Strategy.

4.1.5. Cybersecurity areas

Cyber security areas are defined in accordance with the evaluation of Croatia's priority needs at the time of drafting the Strategy and they cover the security measures in the area of communication and information infrastructure and services, where we have public electronic communications, e-Government and electronic financial services as infrastructure of primary strategic interest for the entire society.

Protection of critical communication and information infrastructure is also a very important area of cyber security. It may be present in each of the three infrastructure areas mentioned above, but has significantly different characteristics and it is necessary to determine the criteria for recognizing those characteristics.

Cybercrime has been present in the society for a long time in different forms, but at today's level of development of the society's virtual dimension it poses

a constant and growing threat to the development and economic prosperity of every modern state. That is why countering cybercrime is also considered a priority cyber security area and it is necessary to define the strategic goals to improve the efforts in countering this type of crime in the coming period.

The area of cyber defence represents the part of the defence strategy falling under the responsibility of the ministry in charge of defence issues. It is the subject of separate elaboration and action, which will be pursued using all the necessary elements arising from this Strategy. Cyberterrorism and other cyber aspects of national security are dealt with by a small number of the competent bodies within the security and intelligence system and require a separate approach, and that will also include the use of all the necessary elements arising from this Strategy.

Cyber security areas are analysed in relation to the general goals of the Strategy in order to identify the special objectives aimed at achieving improvements in each individual area and the measures necessary for achieving the goals of the Strategy. The special objectives, as well as the measures that will be further elaborated by the Action plan for the implementation of the Strategy, are determined with regard to the defined society sectors and the influence of the cyber security area on each individual sector, but also with regard to the forms of mutual cooperation and coordination of cyber security stakeholders. The principles defined by the Strategy are followed in the elaboration of the cyber security areas.

It is logical to predict that vulnerability of geospatial data is expected to be potentially and ultimately targets for physical attacks on objects within the data (e.g. changing the metadata with false information within the georeferenced data).

4.2. Implementation of the Strategy

Action plan for the implementation of the Strategy, made for the purpose of implementing the Strategy, elaborates the defined strategic goals and determines the implementation measures necessary for achieving those goals, along with the competent authorities and the list of deadlines for their implementation.

Action plan for the implementation of the Strategy allows for systematic oversight of the implementation of the Strategy and serves as a control mechanism which will show whether a certain measure has been implemented in its entirety and has produced the desired result, or it should be redefined in accordance with the new requirements.

In order to determine in due time whether the Strategy is achieving the desired results, namely if the defined goals are being accomplished and the established measures implemented within the planned time frame, it is necessary to set up a system of continuous monitoring of the implementation of the Strategy and Action plan, thus also setting up a mechanism for coordinating all the competent government bodies in creating the appropriate policies and responses to threats in cyberspace.

For the purpose of reviewing and improving the implementation of the Strategy and Action plan for its implementation, the Government of the Republic of Croatia will establish the National Cyber Security Council[1] (hereinafter "the National Council"), which will

(1) systematically monitor and coordinate the implementation of the Strategy and discuss all issues relevant to cyber security;
(2) propose measures to improve the implementation of the Strategy and Action plan for the implementation of the Strategy;
(3) propose the organization of national exercises in the area of cyber security;
(4) issue recommendations, opinions, reports and guidelines related to the implementation of the Strategy and Action plan, and
(5) propose amendments to the Strategy and Action plan or propose the adoption of a new Strategy and action plans, in accordance with the new requirements.

Based on the requirements described in the area of cyber crisis management, the National Council will

(1) address issues essential for cyber crisis management and propose measures for higher efficiency;
(2) analyse the reports on the state of security submitted by the Operational and Technical Cyber Security Coordination Group;
(3) issue periodic assessments of the state of security;
(4) define cyber crisis action plans;
(5) issue programmes and action plans for the Operational and Technical Cyber Security Coordination Group and direct its work.

To ensure the support for the work of the National Council, the Government of the Republic of Croatia will establish the Operational and Technical Cyber Security Coordination Group,[2] which will

(1) monitor the state of security in national cyberspace for the purpose of detecting threats that may result in cyber crisis,
(2) issue reports on the state of cyber security,
(3) propose cyber crisis action plans, and
(4) perform other duties according to the issued programmes and activity plans.

The representatives in the interdepartmental body, the Operational and Technical Cyber Security

Coordination Group, mutually ensure access to operational information from their scope for the purpose of coordinated action during cyber crises.

The entities tasked with the measures from the Action plan for the implementation of the Strategy are responsible for monitoring and collecting information on the implementation and efficiency of the measures and are required to submit consolidated reports to the National Council once a year, no later than the end of the first quarter of the current year for the previous year or, if necessary, more frequently, namely at the request of the National Council.

The National Council will submit the reports on the implementation of the Action plan for the implementation of the Strategy to the Government of the Republic of Croatia no later than the end of the second quarter of the current year for the previous year.

The Strategy will be revised after three years of implementation, based on the reports of the entities tasked with the measures from the Action plan for the implementation of the Strategy. The National Council shall submit to the Government of the Republic of Croatia a consolidated report with the proposed amendments to the Strategy no later than the end of the year of revision.

5. Results of the action plan implementation strategy

5.1. Generally

Strategy and Action Plan were adopted on 7.10.2015 (NN number. 108/2015). The National Council and Operational-Technical Coordination for Cyber Security (NN number 61/2016) have been established for the implementation of the prescribed goals (general and special) and measures.

The original data for 2016 were collected in a standardized form (questionnaire) by filling in the Questionnaire of all relevant cyber security officers in the Republic of Croatia (30 institutions). Questionnaires required metrics of deadlines and specifically indicators of implementation. Reports on Implementation of the Action Plan for the Implementation of the Strategy in 2016 have been submitted and the last published Annual Report on the Implementation of the Action Plan and the Strategic Security Strategy on the Government of the Republic of Croatia website (57th Session, Publication 22.09.2017) [14]. We personally participated in the drafting of the Strategy and the Action Plan, as well as in public discussions, round tables, and the collection, processing and analysis as well as in the publication of data and results. In the work on the preparation of the annual report, 40 relevant cybernetic security stakeholders are involved in the Republic of Croatia.

The sample was representative as it covered 30 relevant institutions that are critical to cyber security in the Republic of Croatia, collected and processed data relate to 77 measures for 5 areas and 4 links to the cyber security area specified in the Action Plan and Strategy.

The data were collected on a scientific basis. Previously mentioned (i.e. received) data were processed using qualitative analytical methods.

Using scientific findings based on qualitative analysis, from the collected data, we were able to formulate and present the results.

The data collection methodology allows continuation of experimental research that will be repeated sequentially. The applied methodology is used for a comprehensive assessment of cyber security in the Republic of Croatia.

5.2. Analysis and results of measures implementation

The processed data relate to 77 measures (33 measures in the areas and 44 measures in the area links) listed in the Action Plan supporting a total of 35 specific and 8 general goals in the Strategy elaborated for 5 areas and 4 links of cyber security. Collaboration is the interconnectedness of the implementation of measures with specific and general goals.

A reference model has been developed for approaching and drafting the Strategy and Action Plan and for some countries in the region (e.g. the Republic of Slovenia). The approach was systematic, compliant coherent and comprehensive.

An example of a global campaign of WannaCry's malicious code was also analysed with regard to estimates, i.e. reduction of damage and learned lessons.

All measures of the Action Plan have defined implementation indicators, and the reporting format has enabled four degree readings on the status of implementation: fully implemented / implemented, implemented / carried out, implemented / implemented to a lesser extent or implementation not started.

After processing the data from the accompanying reports of individual measures, out of the 30 relevant cyber security institutions in the Republic of Croatia and the analyses carried out in certain areas and links of the areas defined in the Strategy's objectives and implementation of the Action Plan, the results are as follows:

a) for the following areas:

(1) Public Electronic Communications (3 measures): the Strategy has defined three goals, and the Action Plan identified three measures. Implementation indicators: two measures with a 12-month implementation deadline (since the adoption of the Strategy) and one long-term measure,

(2) Electronic management (8 measures): the Strategy has defined three objectives, and the Action

Plan has developed 8 measures, both sequential and dependent, with descriptive concrete indicators of implementation and set implementation deadlines. Reporting on the implementation of measures in this area 2016 report is absent. The key problem is the insufficient link between technological development strategies and projects in the area of information technology with security strategies and requirements,

(3) Electronic financial services (4 measures): the Strategy has defined two strategic goals in this priority area, and Action Plan 4 measures the specific implementation indicators and deadlines that have already been implemented. The submitted reports have shown that the measures are being implemented, but not fully realized,

(4) Critical Communication and Information Infrastructure and Crisis Management (13 measures): critical communication and information infrastructure are those communication and information systems that manage critical infrastructure, or are essential to its functioning, regardless of which critical infrastructure sector is concerned. In order to protect processes that are crucial to the functioning of the state and economy, the Strategy has defined five goals. To achieve these goals, the Action Plan foresees the implementation of 13 measures. The Council established a working group of the Council for the Implementation of the EU NIS – European Union Directive on Security of Network and Information Systems (NIS Directive) on measures for a high common level the security of network and information systems across the EU from 6 July 2016. For these functionalities, it is foreseen to establish national Competent Authorities for 7 EU critical infrastructure sectors envisaged by the EU NIS Directive. and

(5) Cybernetic Crime (5 measures): the Strategy outlined five objectives, and the Action Plan foresees 5 measures, which, given their character, need to be implemented on a continuous basis.

Total areas have: 33 measures.

b) For area links:

(1) Data Protection (6 measures): the Strategy has identified five objectives and the Action Plan envisages 6 measures, one measure being implemented on a continuous basis, for 4 measures 12 months or 24 months from the adoption of the Strategy or the beginning implementation, while the implementation of one measure depends on the adoption of EU directives,

(2) Technical Coordination in Computer Security Incidents (5 measures): the Strategy sets out three objectives, and the Action Plan for the achievement of these goals has provided for 5 measures, one of which is to be implemented 12 months after the adoption of the Strategy, while the remaining should be carried out continuously,

(3) International Co-operation (6 measures): the Strategy has set 6 objectives and the Action Plan foresees 6 measures for the achievement of these goals, for which continuous implementation and

(4) Education, Research, Development and Enhancement of Cyber Security (27 measures): the Strategy defines three objectives, and the Action Plan has 27 measures for the achievement of these goals, out of which for 3 measures have implementation deadline 2017–2018., and for 2 measures 6 months or 12 months from the adoption of the Strategy, while the remaining 22 measures should be implemented on a continuous basis.

A key issue is the need for much greater consistency of cyber security, and better training of lecturers at different levels and types of education.

Total area links have: 44 measures

There are 77 measures in total.

From the above results it can be concluded that the Strategy 2016 was realized in accordance with the possibilities or engagement of all the stakeholders appointed by the Coordinator and the Council, through the implementation of the Action Plan measures that support the specific and general objectives of the Strategy.

5.3. Conclusion on results

Most of the institutions, in the capacity of the individual Action Plan measures, of which the Council requested the filling in of the form, carried out their obligation and provided the necessary data for analysis to the Council.

The beginning of the implementation of the Action Plan in 2016 has given some results in a large number of 30 joint institutions – cybernetic security stakeholders of various profiles. All institutions – stakeholders have recognized and linked activities within their competence with the thematic conceptual measures of the Action Plan. Certain coordinators of the implementation of the measures have done their job. In order to further implement the national measures in this area, it is necessary to complete the implementation of activities, if necessary with the change of the legislative framework in the area of national critical infrastructure, in order to be able to access the implementation of measures in the area of critical communication and information systems.

A key issue is the need for much greater consistency of cyber security, and better training of lecturers at

different levels and types of education. That is why the results of the cybernetic security education programs being conducted in the Republic of Croatia are questionable.

Developing cyber security within the Strategy and Action Plan should be the framework for the development of all national education programs in this area, and the Council should be involved in the advisory process of the relevant ministry and other bodies related to curricular reform and the improvement of all types and levels of education in the field of cybernetic security and defence in the Republic of Croatia.

5.4. Guidelines for the implementation of action plan measures by the end of 2017

The report points to inadequate horizontal communication between the involved 30 institutions – stakeholders in the implementation of Action Plan measures. It requires the following:

(1) coordinated and targeted implementation of measures for the achievement of general and specific objectives as defined in the Action Plan and Strategy, and stakeholders to further develop their core competences and mutually link and co-ordinate, creating synergistic effects at both national and sectoral levels;
(2) involve other stakeholders in the implementation of measures wherever they can achieve additional quality in the realization of the goals from which the measure comes from.

6. Conclusion and future work

The government has a major role to play in stimulating progress toward higher levels of cybersecurity. Reducing vulnerabilities is the high-leverage area for increasing cybersecurity.

An operations-focused approach is needed. Many government agencies can be used as best-practice examples of enforcing existing regulations.

Limitations of national cybersecurity strategy are related to interrelations and interconnections between many actors at many hierarchical levels.

Nowhere has technological development been more dynamic and comprehensive than in the area of communication and information technology. The focus has always been on the rapid development and introduction of new services and products, while the security-related aspects usually had little influence on the broad acceptance of new technologies.

The life cycles of modern-day information systems, from the process of planning, introduction and usage to their withdrawal from use are very short, which often makes their systematic testing impossible and is most commonly applied as an exception, in expressly prescribed cases.

Users usually have minimal knowledge of the technology they are using, and the technology is applied in such a way that makes it very hard to estimate the security characteristics of the majority of commercial products regarding the protection of user data confidentiality and privacy. Due to that, users' attitude towards the communication and information technology is based almost exclusively on blind confidence.

Modern societies are deeply imbued with communication and information technology. People are nowadays connected using various technologies for the transmission of text, image and sound, including the increasing Internet of Things (IoT) trend.

While a deviation in the normal functioning of a certain kind of communication and information system could go unnoticed, improper operation of some other systems could have harsh consequences for the functioning of the State; it can cause loss of life, damage to health, great material damage, pollution of the environment and the disturbance of other functionalities essential for the proper functioning of the society as a whole.

From the beginning of the development of communication and information technologies until the present day, deviations in their proper functioning have occurred due to different reasons, from human error or malicious action to technological error or organizational omission.

The creation of the Internet and connecting a number of communication and information systems of the public, academic and economic sectors, as well as citizens, created the contemporary cyberspace composed not only of this interconnected infrastructure, but also of the ever growing amounts of available information, and users communicating increasingly among themselves using a growing number of different services – some completely new, some traditional, but in a new, virtual form.

Deviations in the proper operation of these interconnected systems or their parts are no longer merely technical difficulties; they pose a danger with a global security impact. Modern societies counter them with a range of activities and measures collectively called "cyber security".

Based on the vulnerability of geospatial data it may be ultimately logical to expect attacks with physical consequences on objects within the data (e.g. changing the metadata with false information within the georeferenced data).

Further investigations of ours are directed towards finding ends and means in order to enable successful strategy implementation, including new cycle of planning, coordination and control of the action plan fulfilling, including georeferenced data.

Key roles related to that goal have people (actors) and their performance at all levels of national hierarchy (cybersecurity combined with PCS).

Notes

1. Interdepartmental panel composed of the authorised representatives of the competent bodies with national or sectoral policy and coordination responsibilities.
2. Interdepartmental panel composed of the authorised representatives of the competent bodies with operational and technical responsibilities.

Disclosure statement

No potential conflict of interest was reported by the authors.

ORCID

Darko Galinec http://orcid.org/0000-0003-4465-6143

Reference

[1] Cyber Defense. https://www.techopedia.com/definition/6705/cyber-defense. Accessed 2017-02-10.
[2] A. Walls, Perkins E, Weiss J. Definition: "Cybersecurity", G00252816. Gartner Inc.; 2013.
[3] NATO Cyber Cooperative Cyber Defence Center of Excellence Tallin Estonia. https://ccdcoe.org/cyber-definitions.html. Accessed 2017-02-10.
[4] United States Department of Defense. Strategy for operating in cyberspace. Department of Defense; 2011.
[5] Scholtz T. Definition: "People-Centric Security", G00250121. Gartner Inc.; 2013.
[6] *Infosecurity*. http://infosecurityinc.net/wp-content/uploads/2011/07/Consult-Cyber-1Cyber-Threats-Diminishing-Attack-Costs-gaIncreasing-Complexity4.jpg. Accessed 2016-11-15.
[7] Pescatore J. Toward a national cybersecurity strategy, G00167598. Gartner Inc.; 2009.
[8] Herring MJ, Willett KD. Active cyber defense: a vision for real-time cyber defense. J Inform Warfare. 2014;13 (2):46–55.
[9] Marvell S. The real and present threat of a cyber breach demands real-time risk management. Acuity Risk Management; 2015.
[10] Hutchins EM, Cloppert MJ, Amin RM. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. 6th Annual International Conference on Information Warfare and Security; 2011.
[11] Yano ET, Gustavsson PM, Åhlfeldt R. A framework to support the development of cyber resiliency with situational awareness capability. 20th ICCRTS Proceedings: C2, Cyber, and Trust. International Command and Control Institute; pp. 1–11, 2011.
[12] Government of the Republic of Croatia. The national cyber security strategy and action plan for the implementation of the strategy. Official Gazette; 108/2015, 2015.
[13] European Commission, Cybersecurity strategy of the European Union: an open, safe and secure cyberspace, Brussels, 7.2.2013, JOIN 1 final, 2013.
[14] Annual report on the implementation of the action plan and the strategic security strategy on the government of the Republic of Croatia. http://www.uvns.hr/hr/aktualnosti-i-obavijesti/izvjesce-o-provedbi-akcijskog-plana-za-provedbu-nacionalne-strategije-kiberneticke-sigurnosti-u-2016-godini. Accessed 2017-09-26.