THE IMPACT OF THE NATIONAL INFORMATION SECURITY REGULATION FRAMEWORK ON CYBER SECURITY IN GLOBAL ENVIRONMENT

Klaić, Aleksandar; Perešin, Anita

ABSTRACT:

The paper starts from the foundations based on the narrow information security laws and regulations framework within Government sector, covering also the analysis of information from different sectors of society that are dominant from the point of view of information security requirements. These specific information domains include classified and unclassified information, personal data and intellectual property. Further on, the authors research and analyse contemporary state and requirements in the global cyberspace. There have been a lot of changes within security environment triggered by the globalization, technological development and social processes such as liberalization of telecommunications. The term cyberspace is defined in the paper and it is linked with the term of cyber security and put into relation with previously defined national information security regulation framework. Cyber security challenge is viewed as a single, overall, nationally and socially undividable issue, that is based on harmonised requirements between the public and private sector. The paper is based on the concept of information security regulation framework, which is upgraded with the analysis of the cyberspace regulation framework. The results are proposed in the form of the new cyber security regulation taxonomy that includes regulation on cyberspace and regulation on specific information domains. The aim of this paper is to improve mutual harmonisation of many actual regulation processes that deals with cyber security in Government, public and private sectors, and to create common cyber security terminology for communication in global environment.

KEY WORDS: Information security policy, cyberspace, cyber security regulation taxonomy

1. INTRODUCTION

NATO and EU security standards encompass requirements for national information security policy of member states. This is required from all member states and partially from the partner states during cooperation and joint operations. Due to the changes in the contemporary security environment, traditional approach to information security is mostly not adequate. This was especially seen in the world after the end of the Cold War, when globalization and technological revolution in the area of information and communication technologies boomed. Changes in technological capabilities initiated changes in behavior of information system users, as well as in use of classified and other sensitive information and thus getting exposed to new spectrum of threats and vulnerabilities.

Changes in development of technology, liberalization of telecommunication sector, as well as the widespread Internet connectivity, changed the traditional idea of isolation of classified information systems (logical vs. physical isolation) which exposed them to significant vulnerabilities (e.g. software patches updating). Also, to a degree, these processes exposed even

closed information systems to modern threats (e.g. viruses like Stuxnet). Although modern threats could generally be grouped in failures, accidents and attacks, two other important categories of threats emerge contrary to traditional concepts: unstructured threats (hackers, individuals) and structured threats (foreign states, terrorist and criminal organizations). They should be viewed in the context of the post Cold War era and where there are no political and geographical borders for cyberspace. Anonymous criminal perpetrators, fast technology development and numerous inner vulnerabilities, as well as widespread accessibility of cyber attack tools pose new coercion on cyberspace. This result in fact that probability of cyber attacks, as well as other asymmetrical threats, is very hard to predict both on expert analytical and practical level.

Cyberspace, *cyber security* and *cyber terrorism* are parts of cybernetics – science on automatic control systems and generally of processes of control in biological, technical, economical and other systems. Definition of *Cyberspace* (Dunn, 2005) is often similar to the definition of *Information Space* (Klaic and Peresin, 2011) defined as virtual global environment of mutually connected public and private information systems in which data, and specific information that are dominant in the view of information security requirements, are created and transmitted. With this in mind it is very important to apply measures and standards of information security designed to protect confidentiality, availability and integrity of information, as well as availability and integrity of information systems as a whole in which this information is handled, saved or transmitted. Although similar, main difference in terminology arises from the increasing acceptance of terminology based on the word "cyber" so the authors of this paper decided to use the term "cyberspace" instead of "information space".

1.1 Sources, Benefits and the Scope of the Paper

As stated in the introduction, development within cyber security today is focused on prevention and effective reaction to incidents in the cyberspace. The development of cyberspace is based on development of prevention and reaction to incidents as they should be viewed as two mutually connected actions. First step in this process is organization of mutually connected public and private information systems and specific information as previously defined in cyberspace. This includes measures and standards of information security and information security policy in legal entities of society (national information security laws and regulations). Although the access to information security area is somewhat different in different sectors of society, similarities in the environment and threats, in regulatory and business requirements, in methods of approach (through the best practices of information security or risk management),

leads to similar and comprehensive approach to information security in Government and business environment. This approach requires formation of national information security regulation framework that is synchronized with national laws of other NATO and EU states. High-quality concept of national information security regulation framework is the basis for the organized development of cyberspace.

Having in mind widening and complexness of contemporary cyberspace it is necessary to adjust national policy concepts and reorganize required national information security regulation as necessary prerequisites of cyber security development in global environment (Klaic and Peresin, 2011). Problems that may occur in this phase arise from different approaches, concepts and terms that are used in different national environments. This leads to difficulties in process of mutual harmonization of security requirements that are necessary to efficiently combat cyber threats as part of global asymmetric threats.

This paper starts by defining cyberspace and recommends new division of regulation, followed by introduction of clear taxonomy for number of regulation and concepts associated with information security. It points to the key national processes that need to be recognized and regulated in the appropriate and mutually balanced way. The paradigm of cyber security throughout this paper is based on the connections of the well organized fundamental factors of security policy, people, processes and technology (national information security regulation framework), and the well organized environment of newly created cyberspace that connects them (global cyberspace regulation framework).

This paper is based on the concept of national information security regulation framework (Klaic and Peresin, 2011) that is here treated in wider context of cyber security, as the regulation of the specific information domains. Furthermore, it introduces the division of cyberspace regulation. These include systematic differentiation of international and national laws and regulations that set information security requirements or whose demands are met by the use of required controls and standards of information security. Based on initial assumptions on necessity for harmonized information security requirements between Government and private sector, cyber security challenges are viewed within the single, overall, nationally and socially undividable cyberspace. Source of this paper is in the understanding and organization of information (Klaic and Peresin, 2011) and cyber security (Dunn, 2005), as well as in connection of these terms. The paper also relies partially on the research results from the area of compliance management (Hietala, 2008). That is fast developing area due to the large number of requirements for laws and regulations harmonization, especially in multinational corporations.

2. CYBERSPACE AND INFORMATION SECURITY REGULATION FRAMEWORK

In order to get the comprehensive overview of information security regulation framework, that will help us make proper categories of taxonomy division, we analyze three basic information criteria (Klaic, 2006; COBIT, 2012):

1. Security criteria of information (confidentiality, integrity and availability);
2. Fiduciary criteria of information (compliance and reliability);
3. Quality criteria of information (efficiency and effectiveness).

Traditional information security policy is focused on security criteria of information. Contemporary society treats intellectual property (information) similarly to the way market economy treats private property. This means that in modern society, which is undividable from cyberspace, information that are used and exchanged are impossible to isolate. Thus the first thesis of this paper is inability to divide the concepts of information security and cyberspace security. Modern information society leads to use of security, fiduciary and quality criteria of information. Security criteria were adequate to describe closed classified information systems, physically separated from its environment. These systems were completely different from today's closed and open information systems that either communicate or use services from cyberspace in which necessary criteria are also fiduciary (e.g. concept of electronic signature, CA, and PKI) and quality (e.g. service level agreements – SLA).

In the broader terms of cyberspace, the role of information security regulation framework is to set required prerequisites for communication, and to apply the security information criteria on cyberspace and the laws and regulations that define it. Analysis of the dominant information, from the point of view of information security requirements, needs to be viewed from the context of cyberspace in which this information is exchanged. The domains of dominant information from the point of view of information security requirements are [1]: *classified information*, *unclassified information*, *personal data* and *intellectual property*. Intellectual property is viewed in a broader sense as it encompasses copy rights, industrial ownership and trade secret. This paper relates to these information domains as the specific information domains. Basically, it is the enlargement of the information security regulation framework in Government sector (*Fig. 1*) (Klaic and Peresin, 2011), with the regulation of personal data protection and intellectual property protection (national information security regulation framework). The aim of the regulation of the specific information domains is to provide security requirements of different information types, whereas cyberspace regulation provides requirements for communication in cyberspace.

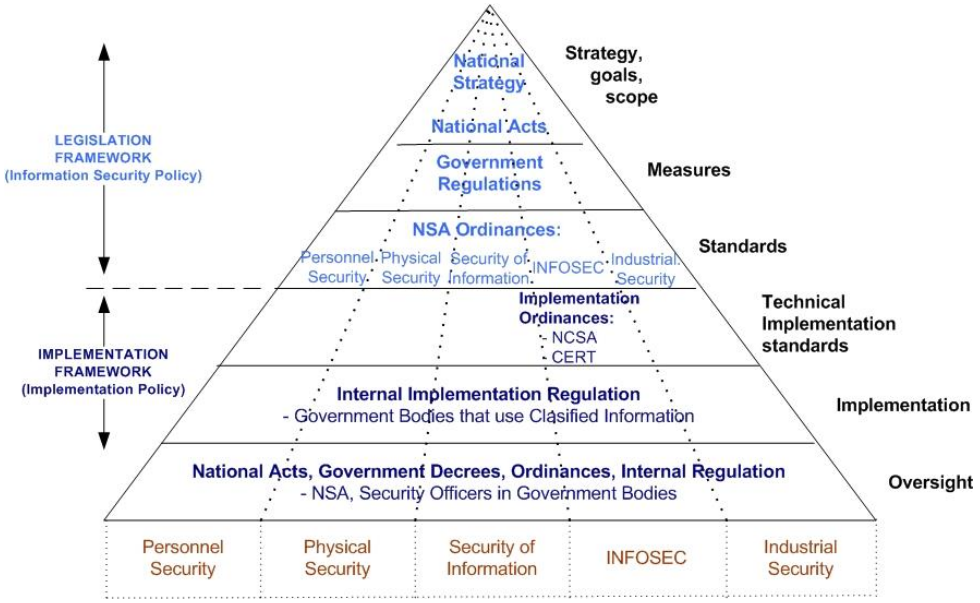

Fig. 1 **-** Information security regulation framework of Government sector in Croatia

3. CYBERSPACE REGULATION

Cyberspace regulation framework is viewed in the context of all three groups of the information criteria. This regulation framework builds upon the regulation of the specific information domains from the Chapter 2, and Government information security regulation as viewed on *Fig. 1*. In this paper we propose the division of cyberspace regulation framework in the following segments, as it is seen on *Fig. 2*:

1. Security regulation,
2. Privacy regulation, and
3. Accountability regulation.

This division stresses mentioned priorities of information criteria. Security regulation primarily deals with security criteria of information. Within the privacy regulation we encompass regulation that deals with fiduciary and quality criteria, whereas accountability regulation deals with liability in cyberspace. Next to stated division, *Fig. 2* shows the regulation of specific information domains that pertains to dominant information types grouped into four categories introduced in Chapter 2 (classified information, unclassified information, personal data and intellectual property).

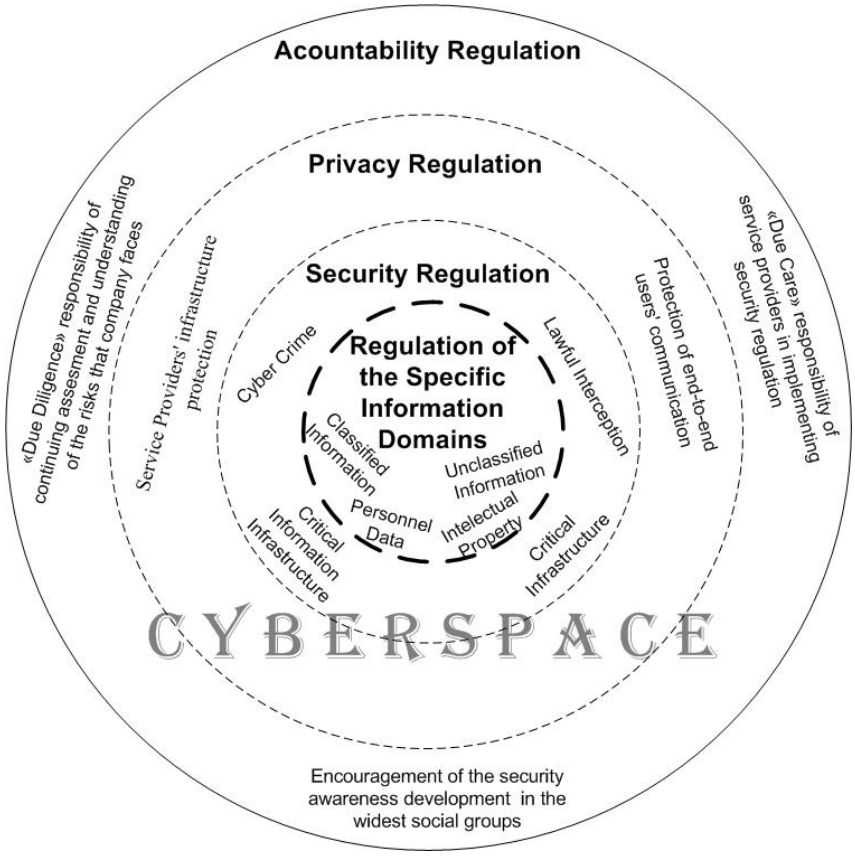

Fig. 2 **-** Cyber security regulation framework

Cyberspace encompasses all vital state entities: Government administration, business, and citizens (GBC). Thus major number of demands placed in front of modern society organization (e.g. citizens ID number, transparency of hospital waiting lists, trade court registry, e-Government services) directly or indirectly relies on cyberspace and confronts with some of the limitations of regulation of the specific information domains. This leads to security requirements of cyberspace. Consequently, with the use of specific information domains in cyberspace, the context in which data is being used is changed, together with the change of threats and risks emerging from mutual interaction of different factors in a public information space. Change of the environment in which we communicate with information, triggers the change of security methodology so that we could achieve our goals defined by the security policy and based on information criteria, so the goals normally don't change.

Despite the fact that the change of cyberspace environment has been lasting for a relatively short period of time, the resulting changes are tremendous and exceptionally significant. For example, during the second half of 1990s, the process of liberalization of telecommunications completely changed the Government approach to hire communication

capacity for classified networks or the approach to the organization of lawful interception of telecommunication services (Klaic and Turek, 2002). Furthermore, creation of e-Government projects open Government administration to citizens and business on the whole new level. It led to development of Internet services, particularly financial services and electronic trade. All these progresses are followed by many initiatives that attempts to control and protect new digital identities and personal data that became ever more exposed to threats from cyberspace.

In order to respond to all these changes in the security environment, regulation framework cannot set the requirements only towards data owners, because they are only the users in the cyberspace, with limited possibility to manage their data within the cyberspace. Regulation framework must set requirements towards the cyberspace itself, actually, towards subjects that creates and use cyberspace, both in the sense of services and infrastructure. The beginning of 21st century, despite the inflation of different national and international regulation, directly or indirectly linked to information security, opens the process of creating improved and more organized cyberspace (EU, 2005; EU, 1995; EU, 2002; EU, 2003).

3.1. Security Regulation

Security regulation provides basic security protection of cyberspace. The development of security component of regulation framework is the primary task of the state administration as it develops information society. Viewed in this way, it represents group of regulation that deals with security threats that emerged as the consequences of cyberspace development. Most significant groups of problems that are defined in this area are *cybercrime*, *lawful interception*, *critical infrastructure* and *critical information infrastructure*.

Cybercrime, computer crime or high technology crime are mostly synonyms that address criminal acts committed through computer technology, as well as criminal acts directly linked to criminal technology or cyberspace. More broadly speaking it includes protection of information and communication privacy, computer business crime, protection of intellectual property, suppression of immoral and illegal contents on networks, and another misuse of information in cyberspace. Cybercrime includes, for instance, unauthorized access to computer system (hacking), computer sabotage, espionage, interception, fraud, counterfeiting, denial of service of information systems, software, audio and audio-visual piracy and other criminal acts connected to digital information media carriers.

Rapid development of technology and electronic services, like electronic trade and e-pay systems, and development of cyberspace in modern society are not adequately supported by criminal regulation and court practices. Because of that in 2001 Council of Europe accepted

Convention on Cybercrime (Council of Europe [COE], 2001). This document represents key and practically unique example of successful Criminal Code harmonization in different states and regions of the world. After it was introduced, Convention was accepted in different states but also enhanced with propositions and practical experiences from cosigning states. Such approach is the basic prerequisite of fighting against cybercrime as perpetrators, victims and the "crime scene" is mostly on different locations throughout the world and under jurisdiction of different national regulation.

Lawful interception is standardized procedure that is used for the interception and acquisition of targeted subscriber communication calls or the information on subscriber calls for persons that are under investigation. The term "call" assumes all types and means of voice and data communication through electronic communication networks covering all type of technologies (voice or data services, switched circuit or IP, fix or mobile telecommunication services). Development of cyberspace caused rapid standardization in the area of lawful interception. Based on the Council of Europe *Resolution on the Lawful Interception of Telecommunications* (Council of Europe [COE], 1995) from 1995, EU standardization body, European Telecommunication Standards Institute – ETSI developed and continued with systematic creation of technical standards and recommendations for lawful interception for all telecommunication technologies. Similar set of standards in the United States is called *Communications Assistance for Law Enforcement Act* - CALEA. This EU Resolution, together with other ETSI standards, represents the way how the states embed control mechanism to cyberspace in order to legally control telecommunication services of individuals by granting access to the information of calls they made or by interception of the content of the calls they initiate.

Critical Infrastructure (CI) is such infrastructure whose dysfunctioning or destruction could weaken national security, economical and social benefits of the nation (Abele-Wigert and Dunn, 2006). Parallel with the development of modern information society during the 1990s, it became known that some of the key sectors of modern society that are vital for national security and economy functioning are based on wide spectrum of mutually connected, national and international information systems, that are used to efficiently and effectively manage certain critical infrastructure. Such Critical Information Infrastructure (CII) supports many elements of critical infrastructure. Because information systems are largely mutually connected or connected to public systems (Peresin and Klaic, 2010) CII becomes ever more exposed to failures, accidents, and problems with different types of malicious accidental or deliberate attacks (viruses, cyber terrorism). Key problem occurs from the fact that attack on CI multiplies the force of attack as relatively small attack on single infrastructural object can have significant

influence and cause damage on all of the connected infrastructural objects (relation between single power plant and energy grid systems). It is needed to mention that source of mutual CI connection can be linked to cyberspace but also to energy, transport or logistics.

Last couple of years EU intensively works on data gathering and analysis of member states national approach to critical infrastructure protection (EU, 2005). *European Program for Critical Infrastructure Protection* (EPCIP) introduced requirements for all EU members (EU, 2006). The prerequisite for the determination of EU CI is the development of national regulation for the protection of national CI. Most of the national initiatives are guided towards the development of early warning systems, such as *EU Computer Emergency Response Team* (CERT) or *Information Sharing and Analysis Centers* (ISAC). Basic criteria for critical sectors determination are national security (telecommunication network, energy, transport, …), economic security (financial sector, production, …), public health and security (water, emergency services, agriculture, …), and the moral of society (special manifestations, national symbols, …). CI is not only physical infrastructure, it also includes services and electronic flow of information, national symbols, and other core values that certain infrastructure gives to society as a whole. Viewed in such way, cyberspace is itself CI and consequently the concepts of CI protection and cyberspace protection are closely connected.

3.2. Privacy Regulation

Privacy regulation provides important aspect of privacy during communication in cyberspace. It represents group of regulation dealing with protection of privacy aimed to develop confidence in users. Most significant groups of problems in the area of privacy protection in cyberspace are *service providers' infrastructure protection* and *the protection of "end to end" users' communication.*

Term of privacy, as seen in this paper, includes personal data of private persons and all other data that their owners', legal and physical persons, estimate to be sensitive and to be used only for selective group of users they are intended for. Service providers' infrastructure protection in cyberspace relates to the application of general measures for personal data protection and standardized requirements for services and infrastructure quality. Furthermore, it defines obligations of electronic service providers on protection of privacy of the users and their services, for instant during automated data processing or international transfer of personal data.

Protection of "end to end" users' communication represents additional security measure used by the end users, most often in coordination with certain electronic services providers (e.g. banks). These services represent the security upgrade of previously mentioned electronic

communication services, in the area of additional checks and protection of users as they access to certain services in cyberspace. It widens security criteria of information for users' interaction in cyberspace by mostly adding criteria such as non-repudiation, authenticity, traceability, and accountability. Services such as Public Key Infrastructure (PKI), Certificate Authorities (CA), as well as individual providers of electronic services (e.g. smart card, token, TAN based authentication solutions) fall under this category.

3.3. Accountability Regulation

Having in mind the importance of cyberspace in society development, considering that the spreading of Internet largely overcomes national cyberspace, and that Internet is accepted in the global society as fully open information media, this all disable the possibility of direct control of cyberspace resources from within the national framework. Management is carried out indirectly through the definition of legal responsibility for security in different business activities connected with cyberspace. Accountability regulation primarily includes the system of responsibility for different aspects of security in conducting business starting from strategic responsibility of top leaders in companies, down to tactical responsibility for the execution of regulation and implementation of security mechanisms to lowering the risks. Elements of this type of regulation are applied to different segments of society from private sectors, individual economic branches (most often financial sector), state sector, to the society as a whole (programs of security consciousness development, data gathering and analysis on security misdemeanors and incidents, cooperation and coordination of different sectors of society in security field etc.), having in mind their role as owners/users of data or owners/users of infrastructure.

Most important group of problems in this area are the "due diligence" concept of responsibility for continuing assessment and understanding of the risks that company faces, as well as the "due care" concept of responsibility of service providers in implementing the security regulation, and the development of security awareness for all end users of electronic services.

Duty of diligence represents the introduction of strategic responsibility for security of business to the board of the company. This concept defines the responsibility of the board of the company for conducting of continuous activities related to the assessment and understanding of different risks of business activities. This responsibility exists for legal persons regardless of its role in cyberspace (user, owner of data, or provider of services). Purpose of such responsibility is the protection of employers, investors, co-workers and clients from the potential losses related

to the exposure to unfitted risks in business activities. This part of regulation, most often within the frame of business sector, is called the regulation of corporate management. Such regulation is so far created only in most developed world countries. Due to the globalization, many multinational global companies are obliged by these requirements as they are registered on the stock exchange in the countries which accepted those regulation (e.g. SOX law in the USA is applied to all companies registered at Security and Exchange Commission - SEC, regardless if they are American or foreign).

Duty of care responsibility lies in the obligation for the implementation of security controls as the countermeasures for recognized risks. With the development and implementation of security policies, procedures and standards, company is secured from possible negligence charges. Except for protection of company from legal negligence consequences, additional attention is given to security in order to stimulate clients who are objectively more secure with the more security aware company. By doing this, lawmakers stimulate the use of electronic services in cyberspace and the development of modern society which leads to array of benefits for the whole state and society. Such requirements are imposed through the different regulation acts, from laws, standards and guidelines, to the service level agreements. Here we can see two different types of responsibility, indirect responsibility for negligence against clients (potential cause of damage to the client), for compromising certain data, and direct responsibility for failing to apply laws and regulations. Responsibility for the implementation of regulation is necessary follow up measure of any regulation, but the specific of information security is in the fact that there isn't 100% security for service provider. That is why it is important for companies to minimize the risk of potential legal responsibility towards users who suffered damages while using some of their services.

Stimulation of security awareness development represents strategic and preventive task of every state that follows modern concepts of society development. Contemporary information society consists of three groups of users: Government administration, business sector and citizens sector (GBC). So far mentioned regulation led to prescribing obligations and responsibilities of subjects in Government administration and business sector. It is clear that these measures protect the end users - citizens. But it is important to additionally protect the end users by preventive measures of awareness development on security threats and risks, as well as appropriate countermeasures that can and should be taken.

Awareness development program is specific because it needs to be adjusted to different group of users in order to give the best possible results. This requires formally developed initiatives regarding security awareness in all three sectors. In Government administration and business sector initiatives and programs are most often part of information security policy and

regular educational program that all employees mandatorily go through. Such programs are most often profiled by the type of working positions and are conducted separately for management and technical staff, as well as for general users in certain company or branch of business, Government administration or group of Government bodies. These programs can be defined by internal implementation acts or by superior acts of security policy (law or other security policy document).

Citizens sector is the only sector indirectly affected by mentioned programs, for example through widely focused educational programs or through the education of Government employees. Directly focused programs and measures are most often conducted by national CERT teams, independent telecommunication regulatory bodies, as well as ministries in charge of electronic services development in public sector.

4. TAXONOMY OF CYBER SECURITY REGULATION FRAMEWORK

Founded on the research results we propose the new taxonomy of cyber security regulation framework, that is based on the national information security regulation framework (regulation of the specific information domains) (Klaic and Peresin, 2011), widened and upgraded by further analysis based on the specifics of cyberspace and introduced in this paper, that interlinks different elements of cyber security (*Fig. 3*).

1 Cyber Security Regulation
- **1.1 Regulation of the Specific Information Domains**
  - 1.1.1 Classified Information
  - 1.1.2 Unclassified Information
  - 1.1.3 Personnel Data
  - 1.1.4 Intelectual Property
- **1.2 Security Regulation**
  - 1.2.1 Cybercrime
  - 1.2.2 Lawful Interception
  - 1.2.3 Critical Infrastructure (CI)
  - 1.2.4 Critical Information Infrastructure (CII)
- **1.3 Privacy Regulation**
  - 1.3.1 Service providers' infrastructure protection
  - 1.3.2 Protection of end-to-end users' communication
- **1.4 Acountability Regulation**
  - 1.4.1 «Due Diligence» responsibility of continuing assesment and understanding of the risks that company faces
  - 1.4.2 «Due Care» responsibility of service providers in implementing security regulation
  - 1.4.3 Encouragement of the security awareness development in the widest social groups

Fig. 3 – Cyber Security Regulation Taxonomy

On the fourth level of taxonomy division, there should be placed actual examples of laws and regulations, ordinances, guidelines and other regulation acts, that regulate some of the

described processes in national or international environment. Taxonomy indicates the most important concepts that globally influence regulation procedures in the area of cyber security and tightly connect the number of factors from information domains, through information security policies to undividable problems of global cyberspace. The aim of the new taxonomy introduction is the use of mutually harmonized terminology to improve mutual communication on global level, as well as to achieve the more consistent approach of all factors of cyber security. It includes all of its subordinate elements such as national, global and international responsibility.

5. CONCLUSION

Analysis of cyber security regulation becomes more and more complex, as ever more laws and regulations directly or indirectly define requirements of information security and cyberspace. Just as prerequisite of market economy development were private ownership and its protection, so the prerequisite of the development of contemporary knowledge economy is intellectual property, and its protection and integrity. From that the need to protect the data emerges, because that data is the very essence of intellectual property. Because of this, the complexity of information security regulation framework will only expand in the future.

Cyber security regulation framework, as seen from the Government point of view, means creation of organized society that is expected to be organized as traditional one. Creation of traditional society regulation lasted far longer than the experience the society has had so far with the creation of cyberspace. This is additional reason for systematical approach to analysis and planning of regulation framework that was suggested in this paper. Looking from the business sector perspective, the state imposes on business considerable burden of compliance with complex regulation framework. In the long term this will enable companies to lower some operational costs through better organization, and lowering security risks and advancing in the management, together with improved quality of services, will develop better market reputation and increase the clients' confidence.

Citizens sector benefits from cyberspace and its security development because information society with traditional society standards improves citizens position within the new information framework. Cyber security regulation framework imposed on the market is also in the function of protecting citizens as the end users that are consequently better protected and delivered better quality services and products. This is possible only when cyberspace and its security are well balanced. The balance is achieved through the careful mechanisms of management and security and clear separation of duties among the owner of data, the owner of

infrastructure and the user. This all requires comprehensive overview and systematic approach to the issue of cyber security and cannot be solved as isolated solutions of some individual problems in cyberspace. It is because such uncoordinated solutions to individual cyber security problems lead to unbalanced processes in cyberspace environment.

This paper represents the model of systematic approach to cyberspace in relation to information security and regulation framework, through categorization of specific information domains and regulation of cyberspace in which this information is being used. The first step in realization of this process is good understanding of existing regulation framework in global environment. Area of compliance management (Hietala, 2008), primarily analyses obligatory regulation for a legal entity, as well as means to more efficiently align its work to existent regulation. This paper, in difference from that suggests taxonomy of cyber security regulation framework aimed to improve overall understanding of needs and better mutual harmonization of future regulation that further globalization of society will bring (Klaic, 2010).

Introduction of a single taxonomy will improve mutual understanding in communication both on national and international levels, but it will also stimulate the development of more consistent approach of all interested players in the area of cyber security.

6. REFERENCES

Abele-Wigert, I., Dunn, M. (2006). International CIIP Handbook. Center for Security Studies: ETH Zurich

COBIT Mapping. Overview of International IT Guidance, 3rd edition. Retrieved January 20, 2012 from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/COBIT-Mapping-Overview-of-International-IT-Guidance-3rd-Edition.aspx

Commission communication COM(2005)229 final of 1 June 2005 to the Council (52005DC0229), the European Parliament, the European Economic and Social Committee and the Committee of the Regions on "i 2010 – a European Information Society for growth and employment". Retrieved January 20, 2012 from http://eur-lex.europa.eu/en/index.htm

Commission decision 2003/375/EC of 21 May 2003 on the designation of the .eu Top Level Domain Registry. Retrieved January 20, 2012 from http://eur-lex.europa.eu/en/index.htm

Communication from the Commission on EPCIP, COM(2006) 786 Final, 12/12/2006. Retrieved January 20, 2012 from http://eur-lex.europa.eu/en/index.htm

Council of Europe. Conventions on Cybercrime. November 2001. Budapest. Retrieved January 20, 2012 from http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG

Council of the EU (96/C 329/01) (1995). Resolution on the Lawful Interception of Telecommunications. Retrieved January 20, 2012 from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996G1104:EN:HTML

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Retrieved January 20, 2012 from http://eur-lex.europa.eu/en/index.htm

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive). Retrieved January 20, 2012 from http://eur-lex.europa.eu/en/index.htm

Dunn, M. (2005). *A Comparative Analysis of Cybersecurity Initiatives Worldwide*. International Telecommunication Union. Retrieved January 20, 2012 from www.itu.int

Green Paper on European Programme for Critical Infrastructure Protection, COM(2005) 576 Final, 17/11/2005. Retrieved January 20, 2012 from http://eur-lex.europa.eu/en/index.htm

Hietala, Jim. (2008). Compliance: Moving Beyond Manual Projects in Silos to an Integrated, Automated Program. *The Compliance Authority Magazine*, 3 (3). Retrieved January 20, 2012 from www.thecomplianceauthority.com

Klaić, A., Turek, F. (2002). National Security and Telecommunications. *International Studies*, 2 (4), p. 97-112

Klaić, A. (2006). Information Security Requirements in the Information Systems Planning Process. Varaždin: Conference Proceedings of the 17th International Conference Information and Intelligent Systems (IIS). Faculty of Organization and Informatics, p. 265-269

Klaić, A. (2010). Overview of the State and Trends in the Contemporary Information Security Policy and Information Security Management Methodologies. Rijeka: Proceedings of the 33th International Convention MIPRO, p. 136-141

Klaić, A., Perešin, A. (2011). The Concept of the Information Security Regulation Framework. 4th International Scientific Conference "Crisis Management Days". Velika Gorica. Book of Papers, p. 678-707

Perešin, A., Klaić, A. (2010). Relation between the Concepts of the Critical National Infrastructure and the Data Protection. Velika Gorica: Book of Papers, 3rd International Conference "Crisis Management Days", p. 13-29