Conceptual Modeling of Information Systems within the Information Security Policies

Aleksandar Klaic and Marin Golub

***Abstract*—In the paper we propose the conceptual modeling of information systems within the framework of contemporary information security policies. The paper presents the basic characteristics and requirements of contemporary information security policies with regard to the similarities of approach among different sectors of society and with regard to the differences comparing to the traditional security approach in the closed environment. Key factors of information security policies: people, process, technology, are increasingly related to the requirements and restrictions imposed on the certain type of information. This is the reason that the approach to the information systems is introduced through the security requirements for information handling, both in the local environment and within the global environment of cyberspace. The important issue of organizational framework is also elaborated, and the modeling process is done with regard to both global and local environment. The approach that is proposed in the paper consists of the elaboration of hierarchical taxonomy of the terms within the defined information security policy domain. It is followed by the analysis of these domain terms with a view to transform them into concepts grouped into subsystems. Finally, these concepts are used to design conceptual model based on the standard UML class diagrams. This formal and structured approach is presented in the paper. It is based on the overview of our research results in the part of information system conceptualization. The research goal is to encompass the influence of the contemporary environment on the information systems and other information security policy factors, in order to use it for the modeling purposes and with the final goal to improve policy planning and implementation processes in different legal and governmental entities.**

***Index Terms*—Conceptual modeling, cyberspace, information security policy, information system, UML model.**

I. Introduction

The paper shows the overview of our research of the contemporary information security policies in the part of conceptual modeling of information systems. The research of the policy field is motivated by the increasing similarities of the information security requirements among different sectors of society today [1]. There are also considerable differences in comparison with the traditional approach to the security in the closed environment. Key factors of the information security policy: people, process, and technology, are increasingly related to the requirements and the restrictions imposed by today's open environment. Complex requirements regarding the approach and the contents of the contemporary information security policies can be seen also through the more frequent use of organizational requirements as another key factor of the policy [2]-[4].

Today, information becomes very important factor of open global environment – cyberspace. The term cyberspace is defined as virtual global environment of mutually connected public and private information systems, in which information, including specific ones that are dominant in the view of information security requirements, is created, handled, and transmitted [5]. This development of technology and society makes the problem of conceptual information modelling within the framework of information security policy to become one of the central problems of contemporary policies. Information is nowadays normally in electronic form, and that form becomes fundamental form that is used throughout the lifecycle of information. From the information security policy point of view, information systems as the basic infrastructure for handling the information have the same importance as the information itself. That is why a number of security requirements for information are related to information systems (e.g. information sharing and information systems interoperability). Of course, the opposite relation is also valid. This means that today's information systems, Internet, and cyberspace influence on the information concepts and that also should reflect the policies [6], [7].

The development of the society and technology, followed by the appearance of new threats and vulnerabilities, leads to the whole range of processes that has similar security influence on both the government and legal entities. First, it was the development of technology and the resulted business processes dependency on information systems and Internet, actually on the elements of cyberspace. Besides that, since the 1990s there were a lot of national processes of liberalization of some sectors such as telecommunications, energy, and transport. That had, and still has, a lot of influence on national security [8]. All this processes led to the changes of people's professional and private lives, deeply influencing them through the social networking sites, different internet services, and the new electronic gadget market. The result is the constant and persistent exchange of information within all parts of our professional and private lives [7]. The similar process of constant and persistent exchange of different information including confidential ones is happening on the level of legal entities. Good example is the area of critical infrastructure protection [9].

II. Contemporary Information Security Policies

Communication needs today regularly demand the

Manuscript received February 14, 2013; revised April 29, 2013.

A. Klaic is with the Office of the National Security Council, Zagreb, Croatia (e-mail: aleksandar.klaic@public.carnet.hr).

M. Golub is with the Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia (e-mail: marin.golub@fer.hr).

exchange of information among different sectors and different legal entities. These needs also cover the approach that has to include the demands for handling specific information domains like personal data or intellectual property. Cyberspace today represent significantly changed environment both in the sense of form, amount, and type of information, and in the sense of different and more complex regulatory requirements. Further on, there is the necessity of international cooperation and global information exchange that leads to added complexity both in the approach and in the content of contemporary information security policies. Such growing complexity looks for the new approaches to facilitate practical solutions in this field. So far, the development of information security policies has been mostly based on the best practices and standardization processes on national and international level. Such approach has offered adequate policy solutions within the organizations local environment [4].

Closed information systems (isolated, air-gap) are decreasingly applicable even in the traditionally closed environments of government classified information systems. Such changes in the environment necessarily demand changes in the information security policy approach on at least two levels. First level is the necessity of the new approach to the policies of information system security in order to fully adapt them to today's open commercial information and communication resources. Second level is the problem of categorizing different types of information within the contemporary environment based on their security criteria [6].

In this paper we present the research results of the mentioned first level of adjustment of policy approach to information system security. This is the part of our wider research project concerning the modeling of contemporary information security policies.

III. Conceptualization of the Information Security Policy Domain – The Scope and the Limitations

Conceptualization of the domain such as the information security policy makes it possible to better associate existing knowledge which is available in different forms. Due to these different forms existing knowledge has relatively weak relations among subdomains from the point of view of information security policy domain. Different forms of existing knowledge are knowledge bases (e.g. threats and vulnerabilities), or procedural knowledge known from the best practises and comprised within some information security standards. According to [10], in order to make specification of conceptualization, or the development of the domain ontology [11], three type of knowledge has to be mapped: declarative knowledge (Know-about Knowledge), procedural knowledge (Know-how Knowledge), and relational knowledge (Know-with Knowledge). Declarative knowledge is represented with the taxonomy terminology, actually the selection of concepts, procedural knowledge is the description of meaning of such concepts, and finally, relational knowledge is represented by mutual relations of the concepts. Recognizing and mapping of the concepts with the goal to develop ontology in the field of information security policy, so far have been mostly focused on explicit knowledge expressed within certain information security standards [12], [13]. In this paper authors are primarily focused on the conceptualization of implicit and tacit knowledge, contained in different policy frameworks, requirements, and standards for the development of contemporary information security policies.

Basically, information security policy represents preventive mechanism. Due to that fact the modeling concepts are focused on external and internal requirements of the policy elements, and the risks are recognized in the model on the level of local environment. Further on, the policy of information security deals primarily with external manifestation of the elements the policy is consisted of. Looking into information systems, external manifestation is the security mode of operation [14], whereas the security models [15] are internal way of functioning of information system that is outside of the scope of the policy as it is treated in this paper. The primary goal of this research is to develop the concepts that cover external manifestations of the elements and the manifestations of the system which is consisted of interconnected elements. Internal way of functioning of certain policy elements is covered in the model through the concepts such as certification and accreditation. The role of the information security policy is to provide the integration of the elements and subsystems regarding their role in the system (model), their external manifestation and interaction with other elements of the system and environment (local and global).

Presented model does not treat separately the business process because the model itself represents the description of the policy as a security process established inside the business process and the business environment. It means that the policy is planned and implemented in the way that it is in line with the requirements and specifics of the business process, whereas the model of the policy is treated the necessary security management process itself.

A. Information Systems Conceptualization

According to the described approach we will more closely look into a few policy areas that are important for the conceptualization of information systems for the purpose of modeling the information security policy.

As it is mentioned, closed sectorial approach to information security, typical for government sector, uses predefined information categories (e.g. classified information) and the obligation to apply a set of protection measures - baseline security measures. We call them security mechanisms to differentiate them from security controls that are the result of risk management in the local environment. Such approach defines previously mentioned requirements for the information systems known as the security modes of operation [14], [16]. Security modes of operation relate factors like trust in computer users (the need and the level of security certification), business process requirements for access to information (Need-to-know), and the requirement for users' authorization (the need and the type of authorization procedure). In difference to security models applied to the design of secure computer system such as Bell-LaPadula [15], today's information systems have to be

analyzed in the significantly more complex environment of cyberspace and significantly more complex role within the business environment. Nonetheless, the basic principle that was used a few decades ago is still applicable and it is used in this paper. That is the principle of differentiating the external and internal manifestations of information systems. In that sense conceptual modeling in this paper follows the way of security modes of operation as external manifestations of information systems. Internal manifestations are taken into account through the conceptualization of certain certification and accreditation procedures.

One of the key differences in the approach to information security during the last two decades is the use of risk management methods as the central concept of the selection of security controls [1]. On the other hand, security mechanisms (baseline security measures) are specifically related to the classified information. Partly, this difference results from the specific criteria applied to classified information by traditional government information security policy, comparing to the more general business assets as the objects of protection in the contemporary information security standards [6]. Contemporary information security policies generally use combined approach in the area of information system security [14], [17]. It means that the baseline security measures are prescribed for the use with the classified information levels, together with the additional requirement to apply certain risk management methods and resulting security controls. Risk management methods within the information security policies of government sector are traditionally used in the fields such as physical security or personnel security. In the field of information system security (different terms are used: *Information System Security*, *INFOSEC*, *Information Assurance* …) ISO/IEC 27001 compatible requirements for the risk management method are mostly used [18], [19]. The similar approach is used in this research project.

Contemporary information sharing requirements look for the possibility of interconnection among the different information systems, and the connection to the Internet and other public services. This requirement is the necessity in both the business and government sectors, but also in between the entities from different sectors [5], [14], [20], [21]. Besides that, the regulation requirements are increasingly applied to the different categories of information that are exposed to the threats of contemporary cyberspace (e.g. personal data, intellectual property) [22]. The requirements for information sharing are not only the part of today's policy practices (*Responsibility-to-Share*) but they are also the legal requirement such as the critical infrastructure protection [9]. Constant and persistent exchange of information through the different commercial communication and information services and resources leads to the creation and storage of different kind of side information that can become security problem for all kind of organizational entities [6], [7]. These aspects of the contemporary requirements of information sharing mostly influence the increasing similarities among the security requirements and information security policies used in government and private sector [6].

Conceptual modeling of information systems security is applied in different papers, such as [23] in which it is applied from the point of view of business process. In [24] it is shown the possibility of information system conceptualization in order to establish security management of information system. In [12] and [13] the conceptualization of some information security standards is proposed. The goal of this paper is to propose the conceptualization of information systems as the part of wider modeling of contemporary information security policies.

B. Contemporary Information Security Policies Modeling

The described security challenges and increased complexity of contemporary information security policies open the need for more formal and structured approach to this complex domain of information security policy. According to [25] the complexity of security environment is the reason why the policy should be looked at in the much wider context than a legal entity is. Such wider view enables the necessary conditions for the proper modeling of security relations in the complex global (national and international) and local environment (legal entity) shown in Fig. 1.

The scheme in Fig. 1, for the purpose of model development, is transformed into four layers that will be analyzed in this paper from the point of view of information systems conceptualization. The environment comprises of all the elements that are controlled through the information security policy of an organizational entity, and all the elements that influence on that entity and its policy. The system comprises of different segments of the information security policies that we call subsystems.

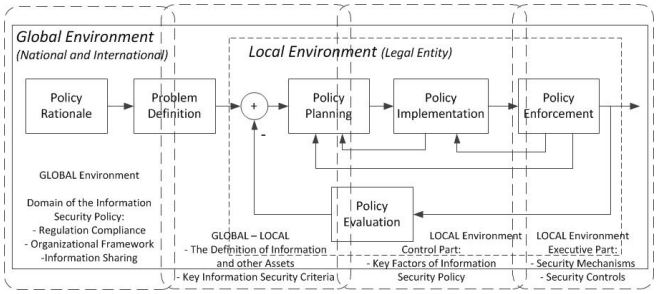

Fig. 1. Lifecycle and the modeling process of the contemporary information security policies.

IV. Taxonomy Development

The hierarchical taxonomy of the information security policy domain is elaborated according to [4], and it is based on the contemporary requirements and restrictions in the handling of different information categories that are necessary both in the government and in the private sector. The taxonomy is treated as the classification schema used for structuring the knowledge in this domain. The elaboration of the taxonomy is done based on the analysis of logical relations among different terms, as well as based on the best practices available in government sector, international organizations, and within some international and national standardization processes. The taxonomy is elaborated with a view to allow future extensions, especially in the executive part of the model shown in Fig. 2. In this paper we present the part of the taxonomy that is related with information systems. The taxonomy is a good base for the definition of common terminology in this multidisciplinary area of information

security policy.

The requirements imposed on the selection of terms within the domain of interest are used according to [26]:

1) Mutually exclusive categories that do not overlap;
2) Exhaustive categories including all possibilities;
3) Unambiguous and clear categories;
4) Repeatability;
5) Logical and intuitive acceptability;
6) Usefulness for the field of interest.

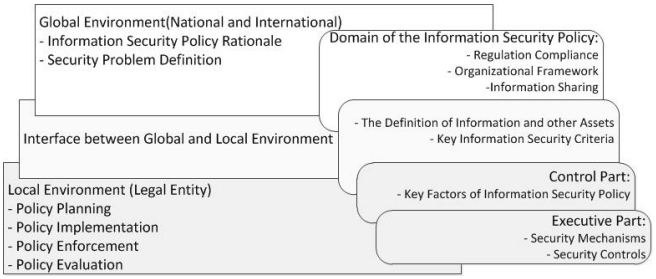

Fig. 2. The model of the contemporary information security policies (high level view).

The structure of the taxonomy is elaborated following these requirements and it is divided into subsystems shown in Fig. 2 (right-hand side). This paper is limited to the overview of the research results within the part of taxonomy that deals with the information system conceptualization. Hierarchical taxonomy is transformed into tabular view of the concepts and subconcepts in order to facilitate the elaboration of taxonomy terms into model concepts. Model concepts have to be recognized both as the categorization and as the mutual relationships of the domain terms. In this way the first part of the recognition of the basic relations among the domain terms is done. These are the groups of the relations of the type such as "is-a" (generalization), "consists-of" (composition), and "contains" (aggregation).

One of the problems in the conceptualization of a model is the use of appropriate tools [25]. Considering the complex and very heterogeneous domain of information security policy we propose the use of standard graphical notation of Unified Modelling Language (UML) [27]. Similar approach is recommended in [28], but with the difference in using modified UML elements. UML comply with the ontology requirements in the sense of class definition and relation notation. UML graphical notation facilitates visualization and understanding of the model and the modelling approach used in this paper.

V. Conceptual Modeling of Information Systems

The model in Fig. 2 consists of a number of subsystems derived from the hierarchical taxonomy of information security policy domain. The modeling goal is further elaboration of relations among the taxonomy terms in order to develop modular ontology as the model, actually meta-model for the development of different information security policy models. The selection of the model concepts depends on the requirements of the global environment (national and international) in the specific case. The instances of the selected concepts will depend on the implementation requirements in the local environment and they will form the local policy of certain legal entity.

In the global environment we primarily manipulate with the information and we primarily differentiate the concept of information type and the level of secrecy of information. In the local environment we primarily manipulate with the information security criteria and the goals of information security. Based on them the security mechanisms and the security controls are selected in order to achieve these goals and criteria. In Fig. 2 this part of information definition and information security criteria is marked as interface between the global (external) and the local (internal) environment. Persons and information systems also depend on the same key criteria (integrity and availability). Additionally, persons have to satisfy the requirements for accessing an information system (confidentiality), and both the persons and the information systems have to satisfy the physical security requirements. The same apply when certain types of information are handled by a person or information system.

The conceptual definition of information systems in Fig. 3 represents the link among the layers of the model in Fig. 2 from the point of view of information system security. The concept of *information system security role* contains four concepts according to Fig. 3. The core elements of the *information system trust* concepts are elements such as (relation "*is-a*"): *information system owner* (link to the organizational entity), *confidentiality level* (link to the information definition), *requirements for the users* (link to the definition of persons), *institutional security roles* (link to the organizational framework), *concepts of identification, authentication, and authorization* (link the persons and information system through the information security criteria), and *security awareness, education and training*.

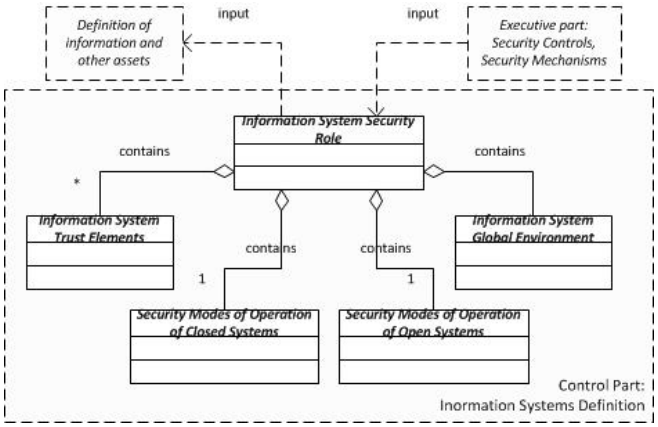

Fig. 3. Basic concepts of the *information systems definition* subsystem shown in UML class diagram.

The concept of *security modes of operation of closed systems* is modeled according to the traditional division [14] into: dedicated, system high, compartmented, and multilevel. The concept of *security modes of operation of open systems* is proposed using the analogy, based on the explanations in section III.A of the paper, and according to the elaboration in [29]. This concept introduces criteria that links together selected factors for open systems: infrastructure, services, and users. Table I shows four levels of trust for open systems, based on the introduced factors that can be internally based (ownership) or externally based (contracts or public availability).

Global environment of information systems is modeled according to Fig. 4. The approach used in model consists of the relation of traditional information security policy elements with contemporary global environment elements [20] [30]. We propose the use of *cyberspace dimensions*: *social dimension* (wider approach to Internet security in general, normally coordinated by National CERT Authority), *economic dimension* (commercial use of national telecommunication resources, normally coordinated by National Regulatory Authority), *security dimension* (e.g. cybercrime, cyber terrorism, organized crime in cyberspace, critical infrastructure protection, normally coordinated by Ministries of Justice or Internal Affairs, Security Services, National Security Authority - NSA, etc.), and *defense dimension* (part of defense policy, cyber dimension of warfare, normally coordinated by Ministry of Defense).

TABLE I: THE ELABORATION OF THE CRITERIA OF SECURITY MODES OF OPERATION OF OPEN SYSTEMS

Trust Level		Implicit	Controlled	Shared	Limited
Inf. Security Criteria		C(S)/I/A	C, I, A		C(P/I/A
Trust Factors	Infrastruct.	I	I	E	E
	Services	I	I/E	I/E	I/E
	Users	I	I/E	I/E	Public
Policy use(IS)	Classified				
	Unclassif.				
	General				

*Markings in the table: I=internal, E=external, C=Confidentiality, I=Integrity, A=Availability, S=Secrecy, P=Privacy, IS=Information System

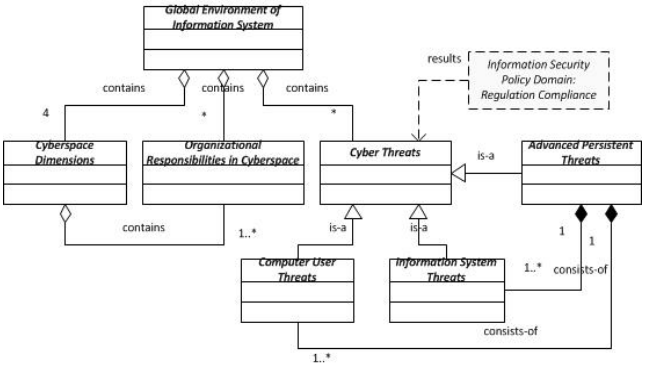

Fig. 4. Elaboration of the concept of *information system global environment* shown in UML class diagram.

Key problem in the cyberspace are *cyber threats*. The information security policy has to assure preventive and protective procedures, but also the procedures in the case of security breaches – reaction and investigation, with possible disciplinary measures or prosecution. From the policy point of view the cyber threats are divided into subconcepts of *computer user threats* (social engineering, phishing, spamming, hoaxes…), *information system threats* and *advanced persistent threats* (APT) as a combination of previous two types. Information system threats use further incident taxonomy according to [26] which differentiate events (action, target), attacks (tool, vulnerability, event, unauthorized result), and incidents (attacker, attack, objective). This concept is related to other concepts in the regulation compliance subsystem of the model.

The part of the elaboration of the concept of information system security principles is shown in Fig. 5. These concepts are part of the security mechanism subsystem (executive part of the model from Fig. 2). The part that is shown in Fig. 5 is the *concept of evaluation and approval of information systems*. It can be seen from Fig. 5 that these concepts from the lower executive part of the model are closely connected with the subsystems in the upper part of the model that define the domain of the policy.

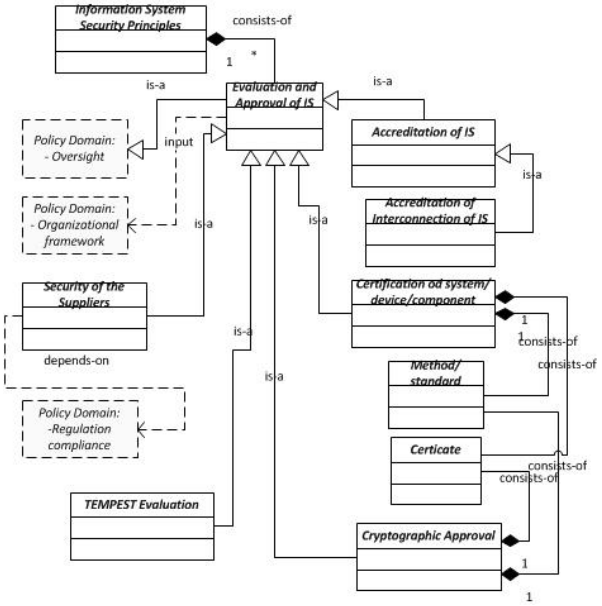

Fig. 5. Elaboration of *the concept of evaluation and approval of information system* (executive part of the model) shown in UML class diagram.

One of the subsystems connected with the concepts on Fig. 5 is the *information security oversight subsystem* from the upper part of the model (policy domain in Fig. 2). Part of the elaboration of that oversight subsystem is shown in Fig. 6.

Besides shown examples of modeling results, in the upper part of the model we have elaborated some other parts of the model such as regulation requirements including security breaches, information system interoperability [6], and organizational framework with the hierarchy of different authorities. The executive part of the model is elaborated following the described approach to baseline security measures, combined with the security controls based on the risk management.

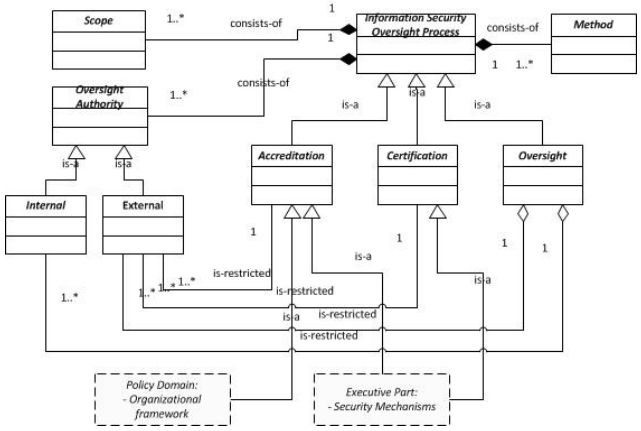

Fig. 6. Elaboration of some of the concepts within *the oversight subsystem* (policy domain) shown in UML class diagram.

VI. CONCLUSION

The goal of the paper is to present the part of our research in the field of modeling contemporary information security policies that is related to the conceptual modeling of

information systems. The approach that is proposed in this research and this paper is based on the formalized and structured approach to the field of information security policy. The main reason for this approach is the increasing complexity of the policy domain. Further research is planned to focus on the elaboration of the complete conceptual model of contemporary information security policies, following the approach illustrated in this paper.

REFERENCES

[1] A. Klaic, "Information security in business and government sectors," in *Proc. 28th Annu. International Convention on Information and Communication Technology, Electronics and Microelectronics - MIPRO*, Opatija, 2005, pp. 193-198.

[2] L. Kiely and T. Benzel, *Systemic Security Management*, Institute for Critical Information Infrastructure Protection, USC Marshall School of Business, University of Southern California, 2007.

[3] R. M. von Roessing, *The Business Model for Information Security*, ISACA, IL, U. S. A. [Online]. Available: www.isaca.org.

[4] A. Klaic, "Overview of the state and trends in the contemporary information security policy and information security management methodologies," in *Proc. 33th Annu. International Convention on Information and Communication Technology, Electronics and Microelectronics - MIPRO*, Opatija, 2010, pp. 136-141.

[5] A. Klaic and A. Peresin, "The impact of the national information security regulation framework on cyber security in global environment," *3rd International Scientific Conference, Corporate Security in Dynamic Global Environment - Challenges and Risks*, pp. 85-96, Institute for Corporative Security Studies, Ljubljana, 2012.

[6] A. Klaic and M. Golub, "Conceptual information modelling within the contemporary information security policies," *36th Annu. International Convention on Information and Communication Technology, Electronics and Microelectronics - MIPRO*, Opatija, 2013.

[7] B. Schneier. (2010). A taxonomy of social networking data. *IEEE Security & Privacy*. [Online]. Available: http://www.schneier.com/essay-322.html.

[8] A. Klaic and F. Turek, "National security and telecommunications," *International Studies II*, pp. 1332-475, vol. 4, Zagreb, 2002, *Centre for International Studies*, pp. 97-112.

[9] A. Peresin and A. Klaic, "The relation between the concepts of the critical national infrastructure and the data protection," *Book of Papers, 3rd International Conference, "Crisis Management Days,"* Velika Gorica, 2010, pp. 13-29.

[10] S. Fenz and A. Ekelhart, "Formalizing information security knowledge," in *Proc. ASIACCS'09*, Sidney, NSW, Australia, ACM, 2009, pp. 183-194.

[11] T. R. Gruber, "Toward principles for the design of ontologies used for knowledge sharing," *International Journal Human-Computer Studies*, pp. 907-928, 1993.

[12] S. Fenz, G. Goluch, A. Ekelhart, B. Riedl, and E. Weippl, "Information security fortification by ontological mapping of the ISO/IEC 27001 standard," presented at Dependable Computing, 13th Pacific Rim International Symposium, 2007.

[13] A. Ekelhart, S. Fenz, G. Goluch, and E. Weippl, "Ontological mapping of common criteria's security assurance requirements," in *Proc. IFIP TC 11 22nd International Information Security Conference (IFIPSEC2007)*, Sandton, South Africa, 2007, pp. 85 – 95.

[14] The Council of the European Union, "Council decision 2011/292/EU of 31 March 2011 on the security rules for protecting EU classified information," *OJ L-141*, May 27, 2011, pp. 17-65.

[15] D. E. Bell, "Looking back at the bell-la padula model," in *Proc. 21st Annual Computer Security Applications Conference, IEEE*, 2005.

[16] The Council of the European Union, "Council decision of 19 March 2001 adopting the Council's security regulations (2001/264/EC)," *Official Journal of the European Communities*, April 11, 2001.

[17] *Security and Privacy Controls for Federal Information Systems and Organizations*, Initial Public Draft, Special Publication 800-53 Revision 4, NIST, US Department of Commerce, February 2012.

[18] *ANSSI*. Expression of Needs and Identification of Security Objectives – EBIOS. *Risk Management Method*. [Online]. Available: http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html, 2010.

[19] BSI. IT Security Guidelines. *IT Grundschutz in brief*. [Online]. Available: https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html, 2007.

[20] North Atlantic Council, "Security within the North Atlantic Treaty Organisation, Corrigendum to C-M (2002)49 dated 17 June 2002, Amendment 9, Declassified - Publicly Disclosed – PDN (2010)0003-ADD1," *NATO*, February 5, 2013.

[21] F. Bicchi and C. Carta. (2010). The COREU/CORTESY network and the circulation of information within EU foreign policy. [Online]. Available: http://www.reconproject.eu.

[22] European Commission, "Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century," *COM (2012) 9 final*, Brussels, 2012.

[23] C. Wolter, M. Menzel, and C. Meinel, "Modelling Security Goals in Business Processes," *Lecture Notes in Informatics*, Modelierung 2008, GI Edition, Gesellschaft für Informatik, Bonn, 2008.

[24] B. Tsoumas and D. Gritzalis, "Towards an Ontology-based Security Management," in *Proceedings of the 20th International Conference on Advanced Information Networking and Applications, IEEE*, vol. 1, pp. 985-992, 2006.

[25] A. Klaic, N. Hadjina, "Methods and Tools for the Development of Information Security Policy – A Comparative Literature Overview," in *Proc. 34th Annu. International Convention on Information and Communication Technology, Electronics and Microelectronics - MIPRO*, Opatija, vol. 5, pp. 190-195, 2011.

[26] J. D. Howard and T. A. Longstaff, *A Common Language for Computer Security Incidents*, Albuquerque, New Mexico, U.S.A.: 1998, Sandia National Reports.

[27] Unified Modeling Language Superstructure. (2009) *Object Management Group*. [Online]. 2(2) Available: http://www.omg.org.

[28] T. Dillon, E. Chang, M. Hadzic, and P. Wogthongtham, "Differentiating Conceptual Modelling from Data Modelling, Knowledge Modelling and Ontology Modelling and a Notation for Ontology Modelling," *5th Asia-Pacific Conference on Conceptual Modelling*, vol. 79, Australian Computer Society, Wolongong, Australia, 2008.

[29] A. Klaic, "Information Security Requirements in the Information Systems Planning Process," *Conference Proceedings of the 17th International Conference Information and Intelligent Systems*, Varazdin, 2006, pp. 265-269.

[30] Information technology – Security techniques - guidelines for cybersecurity. (2012). [Online]. Available: www.iso.org.

A. Klaic received the BS degree (1990) in Electrical Engineering and Computing, MS degree (1997) in Control Engineering and currently is Ph.D. candidate in Computer Science, all at the Faculty of Electrical Engineering and Computing, University of Zagreb. He is working as Assistant Director responsible for information security at the Office of the National Security Council in Zagreb (Croatian National Security Authority - NSA). His interests include information security, systems theory, control theory, and embedded systems.

M. Golub received his BS degree (1992) in Electrical Engineering, MS degree (1996) and Ph.D. degree (2001) in Computer Science, all at the Faculty of Electrical Engineering and Computing, University of Zagreb. Currently he is working as an associate professor at the Department of Electronics, Microelectronics, Computer and Intelligent Systems, faculty of Electrical Engineering and Computing, University of Zagreb. His interests include parallel algorithms, operating systems, evolutionary algorithms and computer system security.