Methods and Tools for the Development of Information Security Policy – A Comparative Literature Review

Aleksandar Klaić*, Nikola Hadjina**
* Office of the National Security Council, Zagreb, Croatia
** Faculty of Electrical Engineering and Computing, Zagreb, Croatia
aleksandar.klaic@public.carnet.hr; nikola.hadjina@fer.hr

Abstract - Information security policy is primarily determined by the environment in which various information are being used and communicated. Such growing complexity of the security environment looks for the appropriate methods and tools for the support of the processes of planning, implementation, and enforcement of information security policy. Comparative review of the available literature is used to analyze the state of the development in this field. Based on that, some observations and a priori hypothesis are given. These hypotheses are then thoroughly checked throughout the more detail analyses of the selected scientific papers. The goal is to determine actual state and trends in the field of methods and tools for the support of processes of planning, implementation, and enforcement of information security policy.

I. INTRODUCTION

Information security policy is primarily determined by an environment in which various information are being used and communicated. The environments, in which different kind of information are used, from the point of view of information criteria of confidentiality, integrity and availability, have been changing a lot throughout the last twenty years. Constant development of new technologies, as well as the social development and globalization, undoubtedly is going to continue that change of the security environments in the future. In accordance with the new technological potentials and societal needs, the new requirements of the users arise. It leads to the situation where it is necessary to use various types of information in various and sometimes completely new security environments, consisted not only of technology, but also of the other two key factors of security policy – people and processes. The change of the societal relations is visible through the range of fields like it is for example: development of business processes, labour mobility, multiculturalism, global fight against terrorism, influence of the international organizations like NATO and EU etc. The change of the societal relations in the mentioned fields and some other fields directly is reflected on the key factors of an information security policy: people, processes, and technology. Such growing complexity of the security environment looks for the appropriate methods and tools for the support of the processes of planning, implementation, and enforcement of information security policy.

II. INFORMATION SECURITY POLICY

Based on the described characteristics of the contemporary society development, the implementation of the information security policy is more and more becoming the necessity in all parts of our society. Due to the mutual dependence of the business and organizational policies (e.g. public-private partnership) very often there is a need to arrange and balance the approach to the information security policy among different parts of the society [1]. Further on, contemporary asymmetrical threats such as terrorist threats or cybernetic threats, clearly points out that any of such global threats cannot be solved by solely the technological solutions. The approach to such threats has to be a multidisciplinary approach, and has to embrace all of the parts of the society that are exposed to such threats. Similar conclusion has also stemmed from the field of information security policy that traditionally tries to embrace the three key factors of the security policy: people, processes, and technology. The rapid development of information and communication technology, leads to the new potentials, but also very often to the new threats and added vulnerabilities [2].

If we look at the described situation from the point of view of engineering branch, the role of engineers in the field of information security is primarily analytical. This means that this role consists of analysis and reasoning of different systems, both organizational and technical, from the security point of view, and with the view to anticipate or modify the behaviour of the system through the implementation of information security policy. The term "policy" here is considered as a control system with which it is possible to accomplish desirable characteristics of the business environment in which certain policy is applied. Due to the described changes in the security environment throughout the recent period of time, there is more and more need to extend the engineering role from the before mentioned analysis role to the more appropriate role in preliminary systems structuring and shaping, prior to security analysis, and in order to make the security solutions possible and appropriate, considering described new security environment (e.g. responsibilities of some key security policy/environment players). This role of the preliminary structuring and shaping generally is considered as a normative role. But the complexity of the security environment place engineers in the role that is more and more normative – rules and regulation

formulation. The reason for that is the creation of the appropriate conditions and proper placing of the security relationships that actually accomplish the traditional analytical role of engineers in this new, rapidly changing security environment. Because of the complexity of the security environment, organizational and technical systems, user requirements and needs, and due to the mutual interconnections of all these factors caused by the globalization of business and new social environment, information security policy subject has to be considered in a much wider context. The best example of that is the expansion of the legal compliance throughout the last decade. This expansion links the requirements of the macro environment (government and global society) and the micro environment (legal entities).

Consequently, the approach to the information security policy must be based on the preliminary structuring and shaping of the wider security environment of the system (macro environment). This should be done both from the organizational and from the technological point of view. The final goal is to accomplish optimal management of the system from the security point of view, economic point of view, and also from the contemporary user requirements point of view, both from within the macro environment and from within the micro environment of specific business subject.

Information security policy planning process in practice is mostly based on the implementation of the existing best practices, available standards, or government sector security policies. In most cases it is either a manual process or partly automated process as it is usually the case with the regulation compliance or technical policies such as information system access control. Consequently, significant part of the information security policy planning process remains unexplored. In addition, within the comprehensive approach to the information security policy area, it is necessary to contemplate the policy in the context of the lifetime phases, which includes not only the planning phase of the policy, but also the implementation and enforcement policy phases [3].

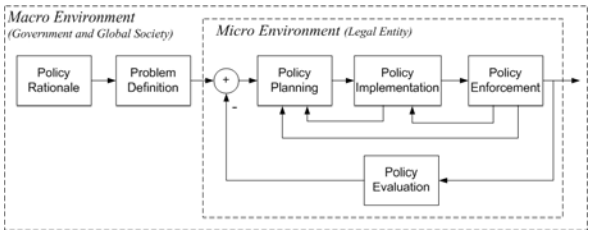

Figure 1. Lifetime phases of the information security policy

The described, comprehensive, lifetime policy approach we present on Fig.1 as a process within the macro and the micro environment. Such approach to the security policy development is very close to the system engineering approach. Many contemporary approaches and methods in the field of information security are based on the system theory [4]. The reasons for bigger contribution and involvement of the engineers in this big picture of the policy development are not only pragmatic, in the sense of better job opportunities in the future, but they are also altruistic in the sense of extending the engineering contribution to the key problems of our time [3]. Finally, the fact is that an information security solution cannot be found exclusively within the world of technology, it is necessary to step out into more comprehensive approach, following all the key factors of information security policy [8].

III. RESEARCH METHOD

A. *The goal of the paper*

The goal of this paper is to determine the actual state of research in the area of methods and tools used in the field of information security policy development, especially in the part of comprehensive approach that includes all key factors of security policy (people, processes, and technology), and covers all phases of the policy lifetime approach according to Fig.1.

B. *The method used in the paper*

Based on the work in [5] and [6], our own customized method is defined. This method is used for the review and comparison of the actual research in the field of information security policy development, focused on the used methods and tools. In order to find available literature we have focused our search on the scientific digital libraries like ScienceDirect and IEEE (www.sciencedirect.com, ieeexplore.ieee.org), and search engines like Google Scholar (scholar.google.hr). Other sources that were used are ACM, WSEAS and Springer libraries of scientific and professional papers (www.acm.org; www.wseas.org; www.springer.com), as well as the libraries available on the Web pages of some universities like Vienna University of Technology, Vrije University Bruxelles, Newcastle, and Stanford University.

For the searching purposes we have used preliminary search strings like: “security policy”, “information security policy”, and added strings like “system theory”, “ontology”, etc. We have made the categorization of the given results according to the publication source (Table I.) and according to the year of publication (Table II.). Based on the previous results in [1], [2] and [4], selected criteria of the literature search (e.g. number of mentions of a term in a paper), as well as the checking of the content of the paper, especially abstract, keywords, and conclusion, the set of papers relevant for this paper has been chosen.

Preliminary hypotheses have been formed based on the previous experience and short overview of the selected papers. These preliminary hypotheses have been verified through the more detailed analysis of the selected papers. The papers are categorized in the groups chosen from the rationale of the information security policy development point of view of this paper. The division into two main categories with subcategories is chosen, as it is shown in Table III. From the set of selected papers some samples are chosen for more detailed analysis. Finally, the qualitative assessment of different directions in this research field, both in the scientific community and in the practice, is given.

In the Table III the categorization of the selected papers according to their content is shown, and an added

analysis of authors' affiliation is introduced by the following sectors:

- S – Universities and scientific institution (all the authors are from scientific community),
- P – Private and governmental institutions (all the authors are from the community of practice),
- SP – Combination of the previous two sectors (authors are from both communities).

The analysis of authors' affiliation in the selected papers gives us the information where the main research projects in this area of research are established.

TABLE I. CATEGORIZATION OF THE SELECTED PAPERS ACCORDING TO THE PUBLICATION SOURCE

Publication Source	Number of Papers
Science Direct	58
IEEE	17
Google Scholar	34
ACM, Springer, WSEAS, Universities	29
Total	**138**

TABLE II. CATEGORIZATION OF THE SELECTED PAPERS ACCORDING TO THE YEAR OF PUBLICATION

Year	Until 2005	2006	2007	2008	2009	2010	Total
Number of Papers	25	13	19	21	38	22	**138**

Further on, within the selected articles the analysis of the used tools has been done. The criterion of the connection between the specific paper and the certain tool is the number of mentions of the term within the paper (occasional mentions such as through the reference titles were eliminated). The number of papers is separately shown with:

- less than three mentions of the certain tool (have the meaning that the paper and the tool are not directly connected);
- three or more mentions (have the meaning that the paper and the tool are directly connected).

IV. PRELIMINARY HYPOTHESIS

Based on the previous work in the field of information security policy research in [1], [2] and [4], and on preliminary comparative review of the available literature, four preliminary hypotheses were defined.

H1: Actual development of the methods in the field of information security policy mostly is based on the system theory.

H2: Significant number of research papers is focused on the technical and narrow purpose oriented security policies, mostly in the field of access control, threats, or vulnerabilities of the information systems.

H3: The ontology applications for the development of methods that has perspective within the process of planning, implementation, and enforcement of the information security policy, represent one of the most important directions of the research and development in this field.

H4: The development of formal and half formal methods in the field of information security policy indicates entering of engineering approach in this field that has been traditionally considered as almost purely normative, especially in the segment of planning. This development is still in the early stage, mostly established within the scientific community.

From the point of view of this paper ontology is considered as explicit specification of conceptualization and it represents the knowledge in formal and structured form [24], [25], [26]. The goals of the ontology usage in the field of information security policy are better communication on security problems, systematic way of knowledge organization and reuse, as well as making progress in reasoning on security problems.

TABLE III. CATEGORIZATION OF THE SELECTED PAPERS ACCORDING TO THEIR CONTENT, AND AUTHORS' AFFILIATION BY INTRODUCED SECTORS

Category of the Paper		Number of Papers	Sector of Authors' Affiliation*		
			S	P	SP
1 Development of information security management methods	**1.1 Strategy**	4	4	-	-
	1.2 Models	19	12	4	3
	1.3 Organization	10	8	2	-
	1.4 Standards	6	5	-	1
1 Total		***39***	***29***	***6***	***4***
2 Ontology applications in the information security management methods	**2.1. Development**	7	7	-	-
	2.2 Models	29	21	4	4
	2.3 Technical and narrow purpose oriented policies	21	14	4	3
	2.4 Standards	20	15	2	3
	2.5 Applications	22	16	2	4
2 Total		***99***	***73***	***12***	***14***
TOTAL		**138**	**102**	**18**	**18**

** **S** – Universities and scientific institution, **P** – Private and governmental institutions, **SP** - Combination of previous two sectors*

V. OBSERVATIONS

Method of searching the literature carried out in this paper was limited by the availability of digital libraries of papers at the moment of search. So the search covered the available digital libraries but also the different literature available to the authors during the previous research of this area of information security policy, mainly in the period of time from 2005 to 2010. Based on the fact that it was rather long period of researching this area (main contributions were made at that time according to the Table II), and also based on the fact that it was relevant amount of digital libraries available (Table I), we consider the sample of literature available for this paper relevant for the goal of this paper.

From the Table II it can be observed that the largest number of papers relevant for this research, around 80%, were found during the last five years, from 2006 to 2010. This is especially noticeable in the field of ontology applications in the information security area (around 70%

- Table III). Further on, around 74% of papers were created within the universities and scientific institutions, whereas less than 13% were created in cooperation with authors from the governmental or private institutions, and only less than 13% were created exclusively by authors from the governmental or private institutions.

A. Preliminary Hypothesis Verification

In the preliminary hypothesis H1 it is claimed that the actual development of the methods in the field of information security policy mostly is based on the system theory. This hypothesis generally is derived from the previous research in [4], but also from the selected papers shown in Table III under sub-categories 1.2 and 1.3. In the next few examples we will show a few different ways of using the system theory in this field of research.

As illustration we can take the approach that is used in the model based on the SABSA security architecture [7]. This model is primarily focused on the protection of defined business values – attributes, that represents desirable characteristics of business values that has to be managed and measured accordingly. In this way the model is at the same time used for the business goals governance and for the management of the security program, because defined attributes cover much wider area than the security requirements are (business and technical strategy etc.). SABSA is comprehensive business system model, and through the implementation of this model existing information security or information technology management standards can be successfully used. The papers in [8] and [9] introduce systemic security model for the information security management. This model includes a new element of organization to the existing elements of people, processes, and technology. Besides that the model includes dynamic interconnections among four main nodes of the model. The main novelty of the model is the clear expression of the attitude that security is consisted of dynamically linked and multidimensional activities [4]. Model based approach to security engineering in the development of programming language for the security modelling is also based on the system theory and the ontology [12]. Further on, in [13], the model of information security governance is elaborated, that is also based on the system theory. The paper in [14] elaborates contemporary cybernetics threats and produces the taxonomy of the main terms that are further elaborated within the process model.

In the preliminary hypothesis H2 it is claimed that the significant number of research papers is focused on the technical and narrow purpose oriented policies, mostly in the field of access control, threats, or vulnerabilities of the information systems. This hypothesis is derived from the previous research in [1], [2], and [4], but also from the selected papers shown in Table III under sub-categories 1.2, 2.2, and 2.3. In the short comment of a few papers we will show a few different examples of technical and narrow purpose oriented policies that illustrate this preliminary hypothesis.

The paper in [15] is dealing with the problem area of information system access control. The paper analyzes this problem area from the position of a development process. The development process is divided into three phases: security policies, security models, and security mechanisms. The authors are focused on programming languages for the access control. The state of policies and models in the contemporary approach to the access control systems is shown together with the usage of XML based programming languages for the access control. The paper in [16] is dealing with the problems area of security configuration of large networked information systems, primarily with the automation of the security rules that are applied to different network elements. Network management based on policy is shown from the point of view of ontology usage. The paper in [17] is the proposal of entering the ontology in the problem area of vulnerability management, with the view to improve the automation of the information security management in the part concerning the usage of existing repositories of vulnerability data. The paper in [18] is focused on the problem area of routing the traffic in the backbones of large networks, where the semantic of the communication between certain network entities is used to drive the application of the relevant security policy on the network elements. The paper in [19] is dealing with the area of cyber forensics, and through the systematic approach it tries to connect the problem areas of cyber vulnerabilities and threats with different parts of society. The taxonomy of the terms is worked out, and the ontology model for the field of cyber forensics is proposed. The comparative analysis of available security ontologies in the literature is shown in [21]. Authors conclude that the majority of the proposed ontologies are focused on the specific domain of interest, or on the problem area of the Semantic Web, and that the more comprehensive usage of ontologies will be the direction of future development.

In the preliminary hypothesis H3 it is claimed that the ontology applications for the development of methods that has the perspective within the process of planning, implementation, and enforcement of the information security policy, represent one of the most important directions of the research and development in this field. This hypothesis is derived from this research and it is illustrated in the Table III by the number of selected papers shown under category 2. Around 70% of selected papers are categorized in this category. Furthermore, as it was briefly mentioned in some of the previous short descriptions of the papers such as: [16] [17] [18] [19] [21], the direction of ontology usage in the field of information security is very diverse (Table III, 2.1–2.5), and covers a huge number of aspects in this field. In the short comment of a few papers we will show some more examples of security ontology applications in the area of information security to illustrate different directions of development.

The paper in [20] analyzes and proposes the architecture of the security management system based on ontology. The importance of the use of security best practices is emphasized in the paper, as well as the necessity of combining these practices with the formalization and conceptualization of knowledge, especially because of the reuse and interoperability properties. In that sense, the usage of ontology represents the framework for the collecting and managing the knowledge of security. The comparative analysis of

available security ontologies in the literature is shown in [21]. One of the conclusions of the paper is that due to the complexity of security area it cannot be formalized with the unique concept. Because of that, the definition of security ontology is not an isolated problem but the necessity of connection of a number of concepts that are in research throughout the scientific community. Further on, it is concluded that the most of the papers in the field of security ontologies are in the early phase of the development and that the proposed ontologies do not have enough formal properties to be reused or extended, and that should be the final goal in knowledge sharing in the information security area. The paper in [22] is dealing with the problem area of ontology mapping with a view to extend the coverage of a single ontology by mapping them with other similar ontologies. Although this area is actively researched, the results are limited and the mapping process is heavily depended on active user participation. As it is shown in [21], this participation of users usually is not simple, even for the security domain experts. It is due to the fact that the developed ontologies are neither enough documented nor completely elaborated, and most of them are in the early stage of the development. The paper in [23] combine the usage of available best practices and standards of information security with the concepts of ontology engineering, developing unified and formal model of security knowledge based on elaborated best practices, with the goal to apply it in the field of security risk management.

In the preliminary hypothesis H4 it is claimed that the development of formal and half formal methods in the field of information security policy indicates entering of engineering approach in this field that has been traditionally considering as normative, and that this development is still in the early stage, mostly within the scientific community. This hypothesis is derived from this research and it is illustrated by previously mentioned papers such as: [7], [8], [12], [14, [16], [18], [20], [23], in which process modelling, logic (reasoning), quantification, or verification are used in place, or in combination with, traditional best practises methods.

Further on, according to the authors' affiliation in Table III, it can be seen that 74% of the papers have been created in the universities and other scientific institutions, and added 13% of the papers have co-authors from the governmental or private institutions. Only the rest of around 13% of the papers have been created exclusively in governmental and private institutions and they are mainly the result of strategic governmental projects or strategic development of huge private corporations. It shows that this area of research is still in the early stage of development mainly within the scientific institutions. Similar conclusion can be found in some references such as [3], [21], and [22].

B. Used Tools

In the Table IV the results of the short analysis of different tools used within the selected papers are shown. All the tools are programming languages or applications, either standardized or widely used. They are ranked according to the number of articles in which they are mentioned, according to the criterion in III.B. Only the term "ontology editor" is a generic term that denotes all the tools of that type and it is left in the table because of the importance of such tools for this area of research.

XML as a concept of programming language is the mostly used throughout different applications in selected papers. The reason for that is its fundamental property of describing unstructured textual information which is the basic problem in different applications of information security policy. As a programming environment, Java environment is the most often used development environment. The most number of programming tools that are generally used in selected papers belong to the different groups of free software tools that are covered with different concepts of licenses for free use and share like GNU or MPL for example. Most of these tools are built against the so-called open standards or recommendations such as the Resource Description Framework – RDF (www.w3.org/TR/PR-rdf-syntax/).

The offer of commercially available tools is present only in the segment of tools that are used in some of the Semantic Web applications (e.g. Jess, Pellet), as well as in some general development environments (e.g. XML, UML). The reasons for the weak offer of commercially available tools for the area of interest in this paper can be explained by the previously mentioned fact that almost 90% of the selected papers were created within the universities and scientific institutions, and also with the previous conclusion that this field is still in an early stage of research. The most of the tools are being developed in the course of the research projects and because of that programming languages are much more used then programming tools.

TABLE IV. TOOLS (PROGRAMMING LANGUAGES/APPLICATIONS) THAT ARE USED WITHIN THE SELECTED PAPERS

Tools*	**OWL**	**XML**	**RDF**	**Protégé**	**UML**	**DAML**	**Ontology Editors**	**SWRL**	**WSDL**	**SPARQL**	**Jess**	**Pellet**
Papers with less than 3 mentions	17	24	17	20	15	13	15	4	7	8	5	1
Papers with 3 or more mentions	51	33	25	16	14	12	1	11	5	4	6	7
Total Papers	**68**	**57**	**42**	**36**	**29**	**25**	**16**	**15**	**12**	**12**	**11**	**8**

* *OWL – Web Ontology Language*
XML – eXtensible Markup Language
RDF – Resource Description Framework
Protégé - open source ontology editor and knowledge-base framework
UML - Unified Modelling Language
DAML - DARPA Agent Markup Language*
** (Defence Advanced Research Projects Agency)*
Ontology Editors- general term for the tools such as Protégé
SWRL - Semantic Web Rule Language
WSDL - Web Service Definition Language
SPARQL - Query Language for RDF
Jess - Rule Engine for the Java Platform
Pellet - Rule Engine Java OWL DL

Ontology editors prevail as the used tools in the selected papers, and the most frequently used tool of this type is Protégé (protege.stanford.edu). OWL (www.w3.org/TR/owl2-overview/) is the mostly used tool within the applications that are based on ontology usage. OWL has a number of advantages similar to XML (platform independence, possibility of describing the textual data), but it is additionally dedicated to the conceptual specifications and connections of terms.

VI. CONLUSION

The results of this research show that the development of the methods for the support of processes of planning, implementation, and enforcement of the information security policy, mostly is relied on the system theory. Technical and narrow purpose oriented security policies, such as information system access control or system vulnerability, prevail in literature. The efforts for the development of novel approaches, methods, and tools, based on the comprehensive approach to the field of information security policy, become more and more significant. The development in this field of comprehensive approach is still in its early stage and it is mainly concentrated within universities and scientific institutions. It is expected in the near future to have more coordinated efforts of collaboration among the researchers from the universities and scientific institutions with the experts from the government and private institutions, especially in the field of novel practical solutions.

Further on, according to our research results, ontology usage can be considered as the most promising direction of development in the field of comprehensive approach to the information security policy. On one hand this development is focused on the system engineering approach to the information security policy. In this approach, the space is opened for a wider role of engineers and engineering approach in this, so far mostly normative area of rules and regulation formulation. On the other hand, the goal of using ontology is focused on systematic evaluation and conceptualization of existing knowledge (best practices and standards), which brings the new tools for developing better models in this heterogeneous field of information security policy.

REFERENCES

[1] Klaić, A., "Information Security in Business and Government Sectors", MIPRO 2005, Conference Proceedings BIS/DE/ISS, p. 193-198, Rijeka, 2005

[2] Klaić, A., "Information Security Requirements in the Information Systems Planning Process", 17th IIS Conference Proceedings, p. 265-269, FOI, Varaždin, 2006

[3] Banares-Alcántara, R., "Perspectives on the potential roles of engineers in the formulation, implementation and enforcement of policies", Elsevier, Computers and Chemical Engineering 34 (2010), p. 267–276, 2010

[4] Klaić, A., "Overview of the State and Trends in the Contemporary Information Security Policy and Information Security Management Methodologies", MIPRO 2010, Conference Proceedings Vol. V. DE & ISS & miproBIS &GLGPS &SP, p. 136-141, Rijeka, 2010

[5] Ma, J., Nickerson, J.V., "Hands-on, simulated, and remote laboratories: a comparative literature review", ACM Computer Surveys, Vol. 38, No. 3, Article 7, September 2006

[6] Ekelhart, A., Fenz, S., Goluch, G., Steinkellner, M. Weippl, "XML security – A comparative literature review", Elsevier, The Journal of Systems and Software 81 (2008) 1715–1724, 2008

[7] Sherwood, J., Clark, A., Lynas, D., "Enterprise Security Architecture", CMP Books, 2005

[8] Kiely, L., Benzel, T., "Systemic Security Management", Institute for Critical Information Infrastructure Protection (ICIIP), 2007

[9] ISACA, "An Introduction to the Business Model for Information Security", 2009, www.isaca.org

[10] CoBIT Standard, V4.1, www.isaca.org

[11] HRN ISO/IEC 27001:2005, HRN ISO/IEC 17799:2005, www.hzn.hr, www.iso.org

[12] Normand, V., Félix, E., "Toward model-based security engineering: developing a security analysis DSML", European Workshop on Security in Model Driven Architecture 2009 (SECMDA 2009), Enschede (The Netherlands), Proceedings p. 22-33, June 24, 2009

[13] Von Solms, R., Von Solms, S.H. (Basie), "Information Security Governance: A model based on the Direct–Control Cycle", Elsevier, Computers & security 25 (2006), p. 408–412, 2006

[14] Knapp, K.J., Morris, Jr. R.F., Marshall, T.E., Byrd, T.A., "Information security policy: An organizational-level process model", Elsevier, Computers & security 28 (2009), p. 493–508, 2009

[15] Vimercati, S.C., Samarati, P., Jajodia, S., "Policies, Models, and Languages for Access Control", DNIS 2005, LNCS 3433, 225–237, Springer-Verlag Berlin Heidelberg 2005

[16] Basile, C., Lioy, A., Scozzi, S., Vallini, M., "Ontology-based Security Policy Translation", Journal of Information Assurance and Security 5 (2010) 437-445, 2010

[17] Wang, J.A., Guo, M., "OVM: An Ontology for Vulnerability Management", CSIIRW '09, April 13-15, Oak Ridge, Tennessee, ACM, 2009

[18] Kodeswaran, P., Kodeswaran, S.B., Joshi, A., Finin, T., "Enforcing security in semantics driven policy based networks", Elsevier, Computer Standards & Interfaces, 2010, www.elsevier.com/locate/csi

[19] Brinson, A., Robinson, A., Rogers, M., "A cyber forensics ontology: Creating a new approach to studying cyber forensics", Elsevier, Digital Investigation 3 S (2006) S37 – S43, 2006

[20] Tsoumas, B., Gritzalis, D., "Towards an Ontology-based Security Management", Proceedings of the 20th International Conference on Advanced Information Networking and Applications (AINA'06), 1550-445X/06, IEEE, 2006

[21] Blanco, C., Lasheras, J., Valencia-García, R., Fernández-Medina1, E., Toval, A., Piattini M., "A Systematic Review and Comparison of Security Ontologies", The Third International Conference on Availability, Reliability and Security, IEEE DOI 10.1109/ARES.2008.33, IEEE, 2008

[22] Noy, N.F., "Ontology Mapping", Stanford University, p. 573-590, "Handbook on Ontologies", Staab, S, Studer, R., 2nd Ed., Springer, 2009

[23] Fenz, S., Ekelhart, A., "Formalizing Information Security Knowledge", ASIACCS'09, March 2009, Sydney, NSW, Australia, ACM, 2009

[24] Gruber, T.R., "Toward Principles for the Design of Ontologies Used for Knowledge Sharing", International Journal Human-Computer Studies 43, p. 907-928, 1993

[25] Guarino, N., "Formal Ontology and Information Systems", Proceedings of Formal Ontology in Information Systems - FOIS'98, Trento, Italy, 6-8 June 1998, Amsterdam, IOS Press, p. 3-15, 1998

[26] Noy, N.F., McGuinness, D.L., "Ontology Development 101: A Guide to Creating Your First Ontology", http://smi-web.stanford.edu/pubs/SMI_Abstracts/SMI-2001-0880.html, 2004

[27] Anderson, R., Bohme, R., Clayton, R., Moore, T., "Security Economics and the Internal Market", ENISA/Springer, 2008, http://www.springerlink.com/index/wm17078084474v12.pdf