

Cyber World as a Social System

Tuija Kuusisto and Rauno Kuusisto

Abstract The increasing applying of information and communication technology is transforming the society into an unknown ground of the continuously evolving cyber world. This challenges the actors of the society and has increased complexity. The purpose of this chapter is to form a hypothesis about how to identify patterns i.e., emergent phenomena about the cyber world for developing security in the society. The cyber world is considered as a complex adaptive system. A system modelling approach to complex adaptive systems is briefly outlined and a social system model of a society is introduced as a content analysis method to complex adaptive systems. The model is populated with a small set of empirical data to have a preliminary view on the content analysis of the cyber world. The results of the content analysis are patterns, i.e., emergent phenomena of the cyber world. They can be utilized for focusing the more detailed analysis of the cyber world on the most significant issues from the security planning and implementation point of view.

1 Introduction

The global digital business as well as the digitalization of the functions and structures of the society provides a lot of benefits to the government, business, customers and the citizens. However, the increasing applying of information and communication technology is transforming the society into an unknown ground of

T. Kuusisto (✉) · R. Kuusisto
National Defence University, Helsinki, Finland
e-mail: tuija.kuusisto@luukku.com

R. Kuusisto
e-mail: rauno.kuusisto@mil.fi

R. Kuusisto
Department of Mathematical Information Technology,
University of Jyväskylä, Jyväskylä, Finland

the continuously evolving cyber world. This transformation covers all the actors, organizations and functions of the society and influences on the way the systems and processes of the society are constructed and executed. This challenges the actors and has increased complexity. Already most of the functions and services of the society as well as the vital functions are automated and interconnected. The actors are dependent on the confidentiality, integrity and availability of information guiding the functions and services. Information in the cyber world is vulnerable to various security threats. Therefore, the security aspects of information as well as the security of the technology structures and systems holding and containing information have become a major issue.

The cyber world as an endlessly expanding domain offers splendid opportunities for new and in novel way manifesting actors, structures and activities. However, having an access to high level cyber potential is required to become a significant cyber world actor. This potential is typically formed only by the resources of nation states, because it is based on such things as existing prosperity, education system, science and research, as well as international business and trade. Some countries will develop more cyber potential than the others but even the major business organizations need a host nation with high enough resources to create the required potential.

However, due to the existing high cyber potential and interconnection, some of the new kinds of actors of the cyber world will emerge and attract people at least for a while. For example, some of the online shopping and social media providers have succeeded well and political and religious groups have been able to recruit followers by communicating their message in the cyber world. These emergent global actors will bring a lot of cultural issues with a variety and even divergence of values to compete in the minds of people. The interpretations of norms and their value will become more inconsistent and the requirements for developing regulations will remain contradictory. Deeper and wider understanding of the characteristics of the society transforming in the cyber world are needed for improving the security of the society.

The purpose of this chapter is to form a hypothesis about how to identify patterns i.e., emergent phenomena and further on simple rules about the cyber world for developing security in the society. These patterns and rules can be used for understanding and maybe organizing the complexity. First, the main concepts of the cyber world are shortly discussed and the complex adaptive system (CAS) theory (Holland 1996) is referred to increase understanding about the nature of the cyber world. A system modelling approach to complex systems is briefly outlined and a social system model of a society is introduced as a content analysis method to complex adaptive systems. The social system model is based on the theories of social systems (Parsons 1951; Habermas 1984, 1989; Luhmann 1999). The model is populated with a small set of empirical data to have a preliminary view on the content analysis of the cyber world. The results of the content analysis are patterns, i.e., emergent phenomena of the cyber world. They can be utilized for focusing the more detailed analysis of the cyber world on the most significant issues from the security planning and implementation point of view.

2 Concepts

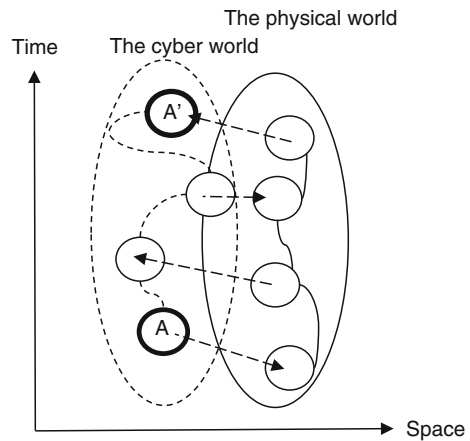
2.1 The Main Concepts of the Cyber World

The concepts and models of the cyber world referred and outlined in this chapter are based on communication philosophy (Habermas 1984, 1989), sociology (Parsons 1951; Luhmann 1999), cognition philosophy (Bergson 1911; Damasio 1999; Merleau-Ponty 1969), organizational culture (Schein 1992; Hofstede 1984), information (Polanyi 1966) and complexity (Holland 1996; Kauffman 1995; Ball 2004). Merriam-Webster (2013) gives a common definition for cyber and defines it as ‘of, relating to, or involving computers or computer networks (as the Internet)’. It can be noted that even if most of the cyber world is constructed of information, the explicit expressions about the electronic information processing aspect of cyber cannot be found on the common definitions of cyber.

This paper uses the concept of cyber world to emphasize the comprehensive nature of cyber. The cyber and the physical worlds are partly overlapping as depicted in Fig. 1. This follows the common human perception about the edge of these two worlds being obscure. For example, supply chain management systems and controlling systems as well as additive manufacturing known as 3D printing consist of constructs and items of the cyber and the physical worlds that are dependent on each other.

One of the definitions for world is ‘the earth with its inhabitants and all things upon it’ and for physical ‘of or relating to material things’ (Merriam-Webster 2013). Based on these definitions, the physical world is defined as the earth with its inhabitants and all things upon it relating to material things. The definitions of world and cyber give the cyber word the following definition: The earth with its inhabitants and all things upon it related to or involving computers and computer networks.

Fig. 1 The relationship between the cyber world and the physical world



As ITU (2011) states the terms cyberspace, cyber environment and critical information infrastructure are used interchangeably. The definition of cyber world is close to the definition of the cyber environment in ITU-T (2008), which says that the cyber environment ‘includes users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks’. Hathaway and Klimburg (2012) present similar thinking when they argue that cyber space contains people and social interaction in the networks in addition to hardware, software and information systems of the internet.

The cyber world includes not only the computers and data and information networks, but also the complete and comprehensive system of human existence in those networks. This interpretation of the concept of cyber world allows to deal with the essential issues and phenomena that emerge from this novel domain. These issues include human social behavior supported by information technical solutions. In this chapter, information and communication technology is considered as an enabler rather than dominator of human existence. This approach allows the studying of the phenomena and characteristics of the cyber world without locking the study on the structural restrictions of any technology.

2.2 The Physical and the Cyber World Framework

A framework for classifying roughly activities of the cyber and the physical worlds is outlined in Fig. 2. The framework supports especially the modelling of activities of the overlapping parts of the cyber and the physical worlds. It can be applied for increasing understanding about how the cyber and the physical world activities are interconnected. In addition, it serves, e.g., as a modeling tool when producing

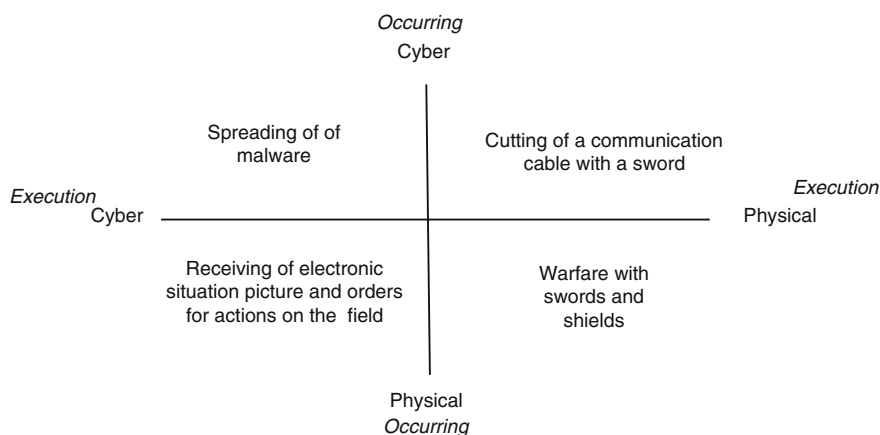


Fig. 2 The physical and the cyber world framework

requirement analysis documents. The framework can be used for assuring that both the cyber and the physical world aspects are concerned.

The framework consists of four fields: physical-physical, physical-cyber, cyber-cyber and cyber-physical fields as presented in Fig. 2. The placing of an activity to one of the fields of the framework depends on the world where the activity is executed and occurs (Kuusisto and Kuusisto 2013). An activity that is executed and occurs in the physical world is placed in the physical-physical field but an activity that is executed in the physical world and occurs in the cyber world is placed in the physical-cyber field. The number of activities executed and occurring only in the physical world is decreasing compared to the activities that are executed or occurring in the cyber world.

Recently, the interest in the kinetic cyber has increased. The kinetic cyber is about the effects occurring in the physical world caused by the activities executed in the cyber world. It is the questions of effects from the technology network to the real world. When this phenomenon is studied further, the following examples can be formed.

Traditional warfare with swords and shields is an activity that is executed and occurs in the physical world. If the warrior disconnects a communication cable with his sword he would perform an activity that is executed in the physical world but occurs in the cyber world. If the warrior has a mobile device and uses it to spread malware on the remaining part of the network he would perform an activity that is executed and occurs in the cyber world. If the warrior receives an electronic situation picture and the orders for the further actions on his mobile device and he would implement the asked actions in the physical battle space there would happen activities executed in the cyber world and occurring in the physical world.

Most crucial in the kinetic cyber are the second and higher order consequential effects caused by damage in cyber related individual entity. The damaging of the power plant stops many other functions almost immediately. Recovery time may be intolerable long causing fundamental or even permanent changes to the existence of the local community or even the society. This, as it, is nothing new. If vital functions and services of the society will fall the society suffers greatly. The new phenomenon is that this damage can be executed distantly and instantly without the physical touch to the target.

3 System Modeling Approaches on the Cyber World

3.1 The Cyber World as a Complex Adaptive System

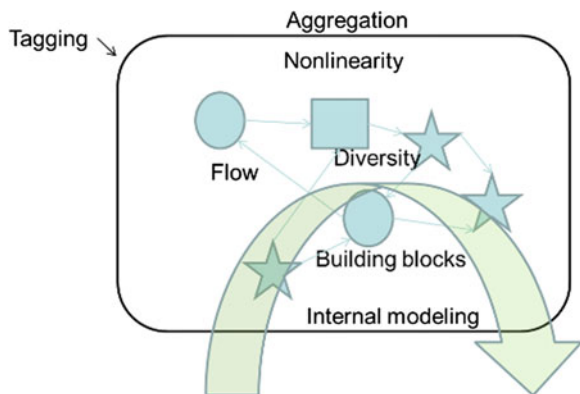
The cyber world is continuously evolving over time. All of the details of the cyber world cannot be known by any groups of actors or by a certain moment of time. These are some of the characteristics of complexity. As Kauffman (1995) and Ball (2004) describe, complexity means that the comprehensiveness of the interacting

entities and processes is not completely or thoroughly known nor under precise, or even any control. Complex systems will emerge outputs that are not necessarily predictable in the content or in time. Complex is not completely known by any group of actors, but it may be understood at least to some degree by some actors. That is different from complicated that is a known but such a big entity that it cannot be described by any individual actor. It can be argued in a simple way that the meaning of complicatedness is relatively degrading while the meaning of complexity is increasing in the cyber world. Complicated phenomenon is deterministically defined, but complex cannot be defined deterministically. However, if the main features and phenomena of a complex system or a system of complex systems are figured out, enough understanding of the behavior principles of this system can be gained.

The complex adaptive system (CAS) theory (Holland 1996) is a widely accepted approach to increase understanding about complexity. It has an actor's point of view to the chaotic nature of a multi-actor interactive system. The CAS theory aims at to explain the adaptive behavior of an entity in its acting environment by categorizing the basic features of the entity. The CAS theory divides the basic elements of an entity in four properties and three mechanisms. A CAS entity with these elements is depicted in Fig. 3. A short description of the elements are:

- (1) An aggregation is a property of an entity. It defines that an entity seeks to categorize similar parts into a class. For example, the parts of vehicles belong to a vehicle class and all the municipalities belong to local government. After the classification the members of those classes are treated as equivalent.
- (2) Tagging is a mechanism that gives a descriptive symbol (name) for an aggregate.
- (3) Nonlinearity is property that expresses that the outcome of the whole is not the sum of its parts.
- (4) A flow is property that tells what transfers between building blocks. A flow can be information, material, radiation or symbol.

Fig. 3 A CAS entity and its basic elements (Kuusisto 2012)



- (5) Diversity is property that tells that a wholeness contains certain (various) amount certain (different) kinds of nodes that have suitable role in that wholeness.
- (6) An internal modeling or a schema is a mechanism that causes certain behavior of an entity, when certain stimulus occurs.
- (7) Building blocks are the mechanism that enables to construct models in a simple way (Holland 1996).

The cyber world can be considered as a complex adaptive system of complex adaptive socio-technological systems. It is neither random nor accidental. It is a collection of systems' elements with certain kinds of universal features and the continuum of their interrelations. This makes the cyber world act in a non-deterministic way that becomes understandable if we perceive the system at the structural level that suits our viewpoint, see Ball (2004), Kauffmann (1995), Moffat (2003). The cyber world cannot be described thoroughly nor defined exactly by the applying of the CAS theories. However, the cyber world can be approached from a purposefully chosen worldview and viewpoint for increasing the high level understanding of its characteristics.

3.2 The Content Analysis of the Cyber World

A system modeling approach for forming of simple rules from the complex systems is depicted in Fig. 4. The modeling process proceeds from the lower left corner to the upper right corner in the figure. The forming of simple rules is based on both the increasing of understanding and the analyzing of the emergently revealing phenomena of the complex systems as well as on the categorizing and analyzing of information collected by utilizing complicated models. This approach was first presented and applied in Kuusisto (2008) in the context of the collaboration support systems.

Complex systems have a tendency to produce emergent phenomena, see Ball (2004), Kauffmann (1995), Moffat (2003). The first step in the modeling process is

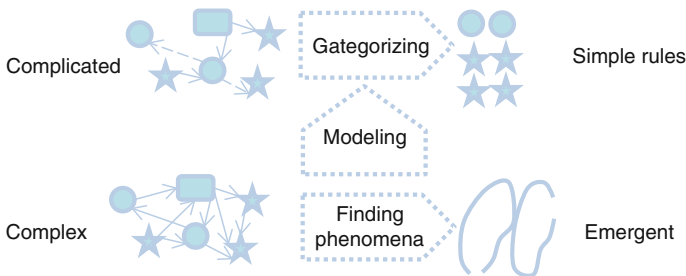


Fig. 4 The content analysis of the cyber world

to figure out these phenomena by approaching the contents of the complex system from a chosen worldview and viewpoint at the structural level that suits the viewpoint. This analysis is performed according to Krippendorff's (2013) content analysis method. The use of the social system model that will be introduced next in this chapter is one method for analyzing the contents of a complex system.

When the emergent phenomena are recognized, they can be utilized for focusing the further modeling of the complex system. This modeling often has to be based on incomplete or fragmentary information and the results of modeling sometimes show themselves as complicated models. However, simple is one component of complex. The complicated models can be simplified by abstracting and categorizing their contents further with the support of the identified phenomena. This produces information for forming of simple rules about the complex system.

The cyber world is a complex adaptive system that inevitably produces some kind of logically understandable phenomena over time. These phenomena can be identified by approaching the cyber world from a chosen worldview and viewpoint. The aim is to find out certain principles of the contents of the cyber world for focusing the more detailed analysis on the most significant issues. This chapter gives an example of finding out the emergent phenomena while the further modeling of the cyber world will remain subject of the further research. The worldview chosen in this chapter is the social system. The primary actors in the cyber world are people so the use of a social system model was chosen as a method to model the contents of the cyber world. The viewpoint of this chapter is the change of the public media focus concerning cyber-related news. Next a social system model is briefly outlined and then the system modeling approach is applied in a media survey.

3.3 A Social System Model as a Worldview to the Cyber World

Social systems have the human perspective on the society. In this chapter it is the chosen worldview to the cyber world. Kuusisto (2004) presents a general social system model based on the thinking of Habermas (1984, 1989) and Parsons (1951). This model is described in Fig. 5, which is derived from a model of organization dynamics presented in Kuusisto and Kuusisto (2009), Habermas (1984, 1989) states that a social system has an initial and a goal state and the communication orientation of the system is internal as well as external as depicted in Fig. 5.

Habermas (1989) refers to Talcott Parsons' (1951) thinking and argues that the information that directs activities of an actor consists of four basic classes: values, norms, goals, and external facts. These are described in the bottom of Fig. 5. The activities using information are on the top of the figure. These are adaptation, goal attainment, integration, and pattern maintenance. The structural phenomena of social systems that consist of culture, community, polity, and institutions are in the

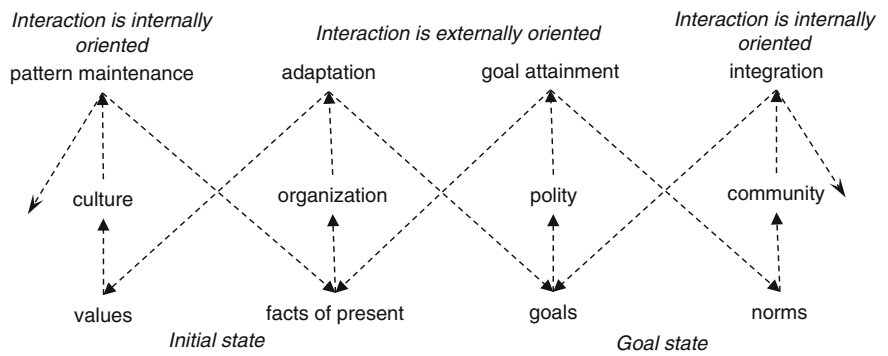


Fig. 5 A system model of a society

middle of the figure. As Habermas (1989) says, cultural systems are more solid than communities, which are again more solid than polity structures and institutions.

Interactivity relationships exist between an item in the Fig. 5 and the items above or below the item. In addition, interaction exists across neighboring action and information items. Pattern maintenance interacts with norms and facts of present, adaptation interacts with values and goals, goal attainment interacts with facts of present and norms and integration interacts with goals and values. So, information of different functional parts of the system is a combination of the influence of neighbor parts of the system and external input of each subsystem of the comprehensive system. It can be easily recognized that this kind of a system is complex thus being emergent.

The cyber world can be considered as a system of social systems. People are acting in the structures of the cyber world guided by the structures of social systems and obeying more or less the internal norms. People acting in the cyber world are producing information both inside a social system and between other, neighboring social systems. This kind of information flowing and continuous emergence of new kinds of interpretations forms a complex system that may be difficult to figure out and that is practically impossible to control. However, the social system model can help to create understanding about the complex nature of the ever interacting and dynamically evolving system of various subparts and phenomena of the comprehensive cyber world thus helping us to figure out relevant enough acts to make it more convenient to live in this kind of new surroundings.

4 The Content Analysis of the Cyber World

4.1 Media Surveys

The system modeling approach was applied in two media surveys in 2011 and 2012. The worldview of these empirical studies was the social system model and

the viewpoint was the change of the public media focus concerning cyber-related news. The structural level the empirical data was collected and analyzed was the state or central government level. The results of the surveys are reported in Kuusisto and Kuusisto (2013). They are one interpretation of the complex cyber world emergent phenomena.

The media surveys show that the cyber world issues are discussed on public but the focus of the discussions is changing over time. The change in the reported cyber-related news (%) according to the categories of the social system model from the year of 2011 to the year of 2012 is presented in Table 1.

The key findings of the first media survey in 2011 include that organization structures were not discussed. This means that it was not known or under general interest that what were the responsibilities and who was responsible of what. Norms and rules were not discussed either. This means that the internal integration of the community had no commonly agreed departure point. That led the society to a situation where the adaptation to the current situation alone was likely to be the driving force of decision-making.

The key findings of the second media survey in 2012 show that the internal discussions in society about the norms and rules of cyber activities and behavior were started. In addition, the external discussions in society about the facts of cyber activities and organization were increased compared to the results in 2011. These results mean that people want to know what kind of norms will guide the world and how the cyber world will be perceived in futures. A strong need to organize the cyber world seems to be in front of us. However, the ways of integration of the various communities is still unclear. This means that the basic question is: Whom we want to let to lead us?

The need to organize the cyber world is likely to be an emergent phenomenon produced from the cyber world. From the security planning and implementation point of view the information about this need can be utilized when implementing the more detailed analysis of the cyber world. This analysis can be implemented by using strategy planning methods such as the analysis of strategic level metrics or by using some of the basic strategy tools like SWOT analysis.

Table 1 The change in the reported cyber-related news (%) in Helsingin Sanomat (2011, 2012) from the autumn 2011 to the autumn 2012

	Interaction is internally oriented	Interaction is externally oriented		Interaction is internally oriented
Action	Pattern maintenance	Adaptation	Goal attainment	Integration
	−3	−4	−11	−1
Structure	Culture	Organization	Polity	Community
	0	5	0	0
Information	Values	Facts of present	Goals	Norms
	1	7	−2	7
	Initial state		Goal state	

4.2 Information Assurance

One aspect on the security planning and implementing is the securing of information. The modern society is dependent on the security aspects of the information guiding the functions and services of the society in the cyber world. Especially, the integrity of information has raised into an important position among information security attributes mutual spectrum. One consequence derived from this is that the information security practices are not anymore sufficient to meet the increasing requirements. Information security can be considered as a phenomenon of a complicated world. Information security strategies, policies, its management principles, priorities and especially toolsets can be determined in a precise way. This is expressed in the various kinds of information security standardization systems too. It may be argued that information security is a mature concept and practice, and it can be practiced in orderly manner quite well in a typical organization.

Alongside information security the concept of information assurance shall be taken under serious consideration. Assurance is typically defined as ‘the state of being sure or certain about something’ (Merriam-Webster 2013). So, information assurance is the state of being sure or certain about information. While information security in its traditional meaning focuses on the information itself in organizations like e.g. enterprises and states and communicates, e.g., societies, information assurance focuses on also security culture, decision-making apparatus, as well as possible activities of human and technological networks and systems. Without a well performing and context relevant information assurance societies, states, coalitions, companies or any other actors cannot fulfill their existence in the spirit of information integrity.

A comprehensive information assurance consisting of strategy, policy and execution, including information security, is needed. This does not mean only the securing of data or making it available, but also the creating of functioning and well enough together understood information assurance culture, decision-making structures, shared critical information as well as structures and functions to put relevant actions in practice. Information is the basic agent to produce relevant action, but it requires relevant structures to become realism. Well planned and proven information assurance is a key factor of that.

5 Conclusions

This chapter presented a system modeling approach for increasing understanding of those phenomena that may be important, when studying the cyber world for developing security in the society. The complex adaptive system theory was applied for understanding the nature of the cyber world and a social system model was introduced as a method to approach the cyber world. The chapter showed how some of the emergent phenomena of the complex cyber world can be identified by using

the social system model. The model was applied for studying the change in the public media focus concerning the cyber-related news.

The system modeling approach seems to support the recognition of the significant issues of the cyber world. However, this approach outlines rough pictures of the cyber world. More exact modeling approaches and methods are needed for producing information that is sufficient for forming of simple rules of the cyber world. These approaches and methods include strategy planning and implementation methods such as metrics analysis. In addition, there is a need for continuing the research work with empirical data collected from several sources and representing longer time periods for verification and validation of the presented system modeling approach.

The results of the media surveys show that the organizing of the cyber world is likely to be in the front of us. It seems that in the current cyber-era the structures of the changing world are unclear. Decision-making apparatus is changing and goals reveal themselves in a different way than before. The global field is becoming more complex requiring new skills for those acting there. Cyber advanced countries, enterprises and social networks have been interconnected together in a non-cancellable way. That interconnected world forms the modern sphere where relevant or even vital activities take place. In a positive future scenario, collectively acting communities reach towards their good future connected together within all areas of exchanging information that guarantees relevant activities.

The changes in the structures and decision-making systems of a society need to be addressed by the security planning and implementation efforts. Cultural systems are more solid than the other structures of a society. Values interact with culture and influence on norms of the society. So, the security planning and implementation activities should be focused on the security culture development and regulation preparation for assuring security in the rapidly changing cyber world. Discussions in the society are needed to be raised for increasing mutual understanding about the interpreting of values concerning security culture and norms covering the cyber world. People will adopt the security culture and accept the norms if the culture and norms are based on the mutual understanding of values. In the long run it seems that the security planning and implementing activities will move on from the regulation preparation to the cyber world community building.

References

- Ball P (2004) *Critical mass: how one thing leads to another*. Heinemann, London
- Bergson H (1911) *Creative evolution*. Henry Holt and Company, New York
- Damasio A (1999) *The feeling of what happens: body and emotion in the making of consciousness*. Harcourt Brace, New York
- Habermas J (1984) *The theory of communicative action. Volume 1: Reason and the rationalization of society*. Beacon Press, Boston
- Habermas J (1989) *The theory of communicative action. Volume 2: Lifeworld and system: a critique of functionalist reason*. Beacon Press, Boston

- Hathaway M, Klimburg A (2012) Preliminary considerations: on national cyber security. Chapter In: Klimburg A (ed), National Cyber Security Framework Manual. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn
- Helsingin Sanomat (2011, 2012) The main daily published newspaper printed in Finland
- Hofstede G (1984) Culture's consequences: International differences in work-related values. Sage Publications, Beverly Hills
- Holland JH (1996) Hidden order: how adaptation builds complexity. Perseus Books, New York
- ITU-T (2008) X.1205: Overview of cybersecurity. ITU-T Recommendations, X Series: Data Networks, Open System Communications and Security. International Telecommunication Union (ITU). <http://www.itu.int/rec/T-REC-X.1205-200804-I>. Accessed 5 Nov 2013
- ITU (2011) ITU national cybersecurity strategy guide. International Telecommunication Union (ITU). <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf>. Accessed 5 Nov 2013
- Kauffman SA (1995) At home in the universe: the search for the laws of self-organization and complexity. Oxford University Press, Oxford
- Krippendorff K (2013) Content analysis: an introduction to its methodology, 3rd edn. SAGE Publications, Newbury Park
- Kuusisto R (2004) Aspects on availability: a teleological adventure of information in the lifeworld. PhD thesis, Edita Prima Oy, Helsinki
- Kuusisto R (2008) Analyzing the command and control maturity levels of collaborating organizations. In: Proceedings of the 13th international command and control research and technology symposium (13th ICCRTS) (Bellevue, Washington, 2008), Paper 028
- Kuusisto R, Kuusisto T (2009) Information security culture as a social system: Some notes of information availability and sharing. In: Gupta M, Sharman R (eds) Social and human elements of information security: emerging trends and countermeasures. IGI Global, Hershey, Pennsylvania, pp 77–97
- Kuusisto R (2012) Information sharing framework for agile command and control in complex inter-domain collaboration environment. In: Proceedings of the 17th international command and control research and technology symposium (Fairfax, Virginia, 2012), p 19
- Kuusisto R, Kuusisto T (2013) Strategic communication for cyber-security leadership. J Inf Warfare 12(3):41–48
- Luhmann N (1999) Ökologisches kommunikation, 3rd edn. Westdeutscher Verlag, Opladen/Wiesbaden
- Merleau-Ponty M (1969) The visible and invisible. Northwestern University Press, Evanston, Illinois
- Merriam-webster online dictionary (2013). <http://www.merriam-webster.com/>. Accessed 9 Sept 2013
- Moffat J (2003) Complexity theory and network centric warfare, DOD command and control research
- Parsons T (1951) The social system. Free Press, London
- Polanyi M (1966) The tacit dimension. Routledge, London
- Schein EH (1992) Organizational culture and leadership, 2nd edn. Wiley, New York (4th edition, Jossey-Bass, 2010)

Cyber Security: Analytics, Technology and Automation

Lehto, M.; Neittaanmäki, P. (Eds.)

2015, X, 269 p. 53 illus., 42 illus. in color., Hardcover

ISBN: 978-3-319-18301-5