2014

Prerequisites for creating resources and compositions for cyber defence

Tuija Kuusisto
National Defence University, Finland

Rauno Kuusisto
National Defence University, Finland

DOI: 10.4225/75/57a84aa8befb8
15th Australian Information Warfare Conference, held on the 1-3 December, 2014 at Edith Cowan University, Joondalup Campus, Perth, Western Australia.

PREREQUISITES FOR CREATING RESOURCES AND COMPOSITIONS FOR CYBER DEFENCE

Tuija Kuusisto, Rauno Kuusisto
National Defence University, Finland
tuija.kuusisto@luukku.com, rauno.kuusisto@mil.fi

Abstract

The aim of this paper is to increase understanding about the prerequisites which evolving cyber society sets for actors, activities and structures of the defenders of society. The research proposes an approach for identifying, analysing and scheduling these prerequisites for decision-making. The paper presents results of two case studies where the proposed approach is applied. The case studies indicate that in the future compositions are needed for forming of joint defence cyber community and resources for joining this community in affordable and beneficial ways. These are the next steps on the strategic path to jointly defended cyber community of global information networks.

Keywords
Systems modelling, complex adaptive systems, information analysis, cyberspace

1. INTRODUCTION

The evolving digitalization of the functions and services of society is shaping the global technological, information, social, business and military networks. The advances in technology including service robots, pattern recognition, big data and the applying of the internet of everything concept provide splendid opportunities for governments and business organizations. Big data approaches accelerate the developing of data analysis methods and approaches both for military and business use. The change in society is not; however, limited to technologies available or to the virtual environments, but it will transfer society to an endlessly expanding, unknown global terrain, where values, norms and objectives often appear as vague and weird. This unknown terrain often hampers attempts for selecting, analysing and scheduling issues to be decided. Wider and deeper understanding is needed about the prerequisites which the changing society sets for actors, activities and structures of military organizations in futures. Novel approaches are required to bridge the gap between the decision-making needs and supplies.

The overall frame of reference of this paper is global information networks as complex adaptive social systems. Derived from the definitions of information and networks as presented in Cambridge (2014) the term global information networks is defined as a large system consisting of parts that are connected together to allow facts of someone or something to be communicated between or along the parts. The term emphasizes the significance of global interdependencies and the continuous flowing of information in cyberspace. These global interdependencies occur in the physical, logical and social layers (US Army, 2010) of cyberspace.

The major actors of the global information networks have an access to the high level cyber potential. This access is required for creating significant resources and capabilities. The high level cyber potential is typically formed only by the resources of advanced nation states, because it is based on the cultural heritage, social structures, existing prosperity, science, research and development, education system and infrastructure as well as international business and trade. Even the major business organizations need a host state or states with high enough cyber potential. A well-functioning public-private partnership often delivers mutual benefits for the both parties. The public organizations provide the access to the high level cyber potential and the business organizations deliver resources and capabilities. Nation states collaborating with global and local enterprises are thus often the most effective cyber world actors.

Military operations are typically classified to strategic, operational and tactic level activities. The relationships between these levels are described in Figure 1. Strategic activities include the setting of the overall objectives and the determining of the path to these objectives or the developing of already chosen paths. In civil organizations, the operational art level activities are often hidden between the strategic and tactic levels. However, operational art or operations art is a widely recognized concept in the military context.

Piatt (1999) studies the concept of operational art as a discipline between the strategic and tactical activities. He argues that operational art is ‘the methodology used to determine how best to apply military resources to

accomplish strategic aims. It consists of operational analysis, design and planning'. US DoD (2013) has the human capabilities perspective on operational art. It defines that 'operational art is the cognitive approach by commanders and staffs--supported by their skill, knowledge, experience, creativity, and judgment--to develop strategies, campaigns, and operations to organize and employ military forces by integrating ends, ways, and means'.

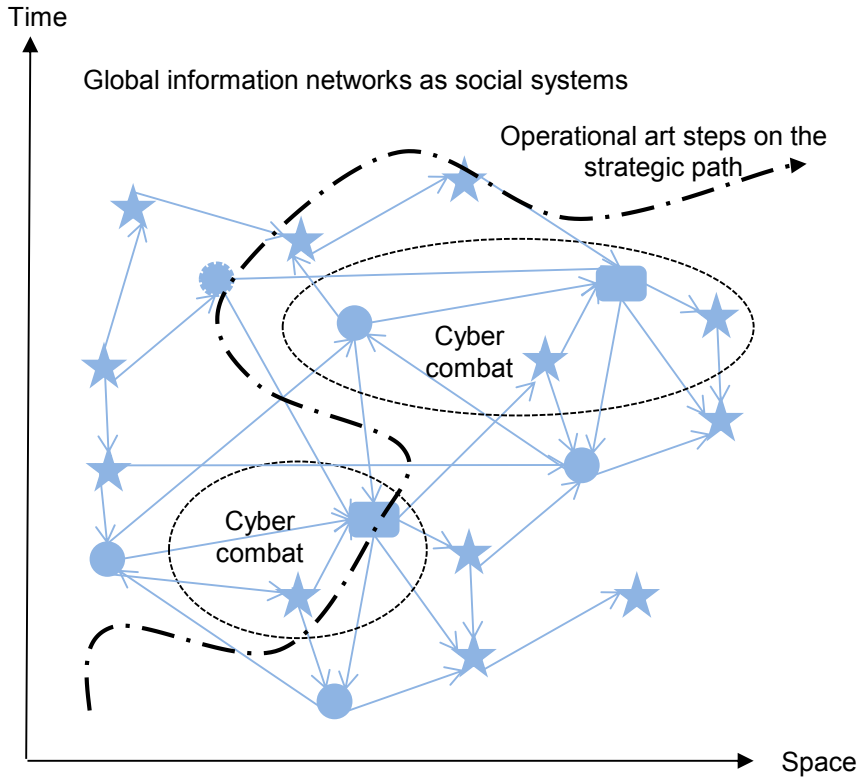

Figure 1. Operational art is selecting steps towards strategic aims and creating of compositions and resources

This paper states that during the operational art phase there is a need to select steps on the strategic path and to create compositions and resources in advance to reach strategic targets efficiently and effectively. Operation art is about organizing and applying of available military forces so that the strategic aims of operations are achieved. If the operational art aspects are not concerned the decision-making about proceeding on the strategic path is often chaotic.

Cyber defence is a common term meaning the preparation and implementation of protective activities against cyber threats. Cyberspace operations are a wider concept meaning 'the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace' (US DoD, 2013). Cyberspace operations include operational art activities. So, they cover selecting steps on the strategic path and creating of compositions and resources in or through cyberspace. Cyber-combats are tactic level activities.

The aim of this paper is to increase understanding about the prerequisites which evolving cyber society sets for actors, actions and structures of the defenders of society. The research proposes an approach for identifying, analysing and scheduling these prerequisites for decision-making. Especially, the research focuses on selecting steps on the strategic path to cyber society and the creating of compositions and resources for effectively and efficiently defending cyber society of global information networks.

2. CONTENT ANALYSIS WITH SOCIAL SYSTEM MODEL

Operational art is a human activity. Social systems approach has the human perspective on the world. Therefore, the social systems were selected as the worldview of this research. Complexity thinking, system modelling, communication and cognition philosophy and sociology was applied to develop the social system model presented in (Kuusisto, 2004) and described in more detail in (Kuusisto & Kuusisto 2009). The model is outlined in Figure 2 and Table 1. From the complexity thinking point of view, the social system model is a complex

adaptive system (CAS) entity (Holland, 1996) having all the properties of that entity. The model is thus a tagged aggregation. The internal modelling of the entity is its division into 12 basic building blocks bolded in Table 1.

The basic building blocks of the social system model and information flows connecting these blocks are derived from Aristotle's, Bergson's (1911), Parsons' (1951) and Habermas' (1984, 1989) thinking. The information flows are shaping the social system. They are depicted with arrows in Figure 2. Information is flowing from values to norms through culture and pattern maintenance and to goals through community and integration and to polity, goal attainment, facts of present, organization, adaptation and finally back to values. In addition, information flows from action to its neighbouring information class and external information enters from facts of present. The external world is influenced by the social system model's actions driven by goal attainment. The model is thus complex and emergent.

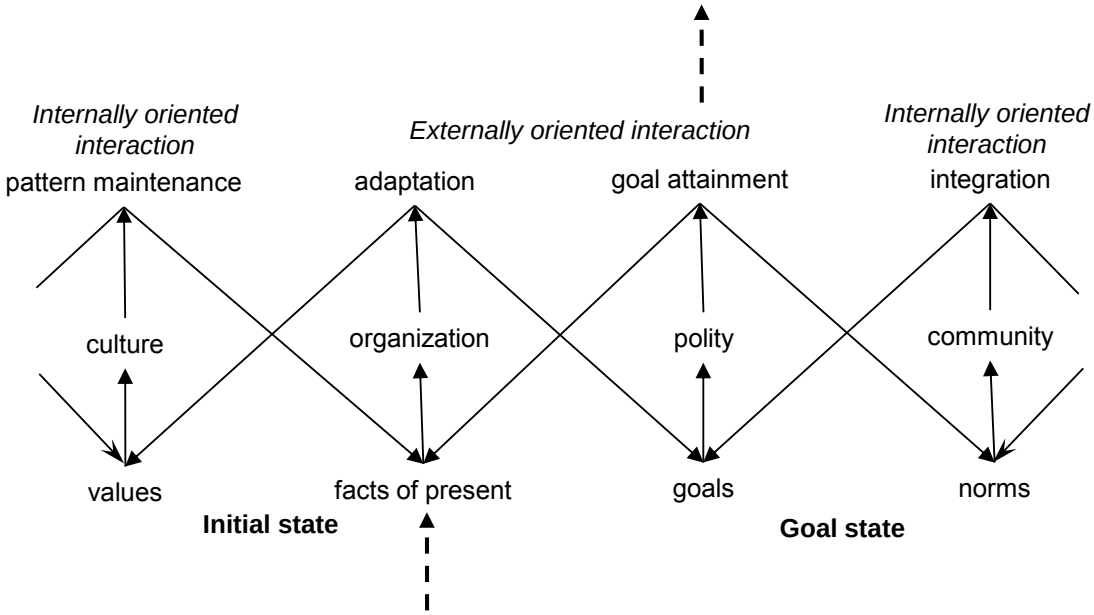

Figure 2. The social system model, based on (Kuusisto & Kuusisto 2009)

Table 1. The social system model with activity hierarchy

	Interaction is internally oriented	*Interaction is externally oriented*		*Interaction is internally oriented*
Action	**Pattern maintenance**	**Adaptation**	**Goal attainment**	**Integration**
	Strategic pattern maintenance	Strategic adaptation	Strategic goal attainment	Strategic integration
	Operational pattern maintenance	Operational adaptation	Operational goal attainment	Operational integration
	Tactic pattern maintenance	Tactic adaptation	Tactic goal attainment	Tactic integration
	Pattern maintenance, operating	Adaptation, operating	Goal attainment, operating	Integration, operating
Structure	**Culture**	**Organization**	**Polity**	**Community**
Information	**Values**	**Facts of present**	**Goals**	**Norms**
	Initial state		*Goal state*	

Information, structure and action hierarchies of complex systems cannot be completely explained nor described. When perceiving a complex system at a structural level such as at a national or defence forces level, the understanding of the hierarchy of actions can be increased by applying a general classification of military

actions. The expanded social system model presented in Table 1 divides actions into strategic, operational art, tactics and operating. The expanded social system model consists of 24 basic blocks, i.e., 8 information and structure building blocks and all the 16 action classes covering actions from strategy to operating.

Global information networks are continuously evolving and the ways cyber operations are implemented are constantly changing. All the details of these networks and cyber operations on them are not known by any actor and they are not under a precise control. These characteristics relate them to complex systems. Complex systems act in a non-deterministic way that becomes understandable when perceiving the system at the structural level that suits the viewpoint. They have a tendency to produce emergent outputs that are not necessarily predictable in the content or in time, see (Ball, 2004), (Kauffmann, 1995) and (Moffat, 2003). So, global information networks and cyber operations will inevitable produce logically understandable phenomena over time. For the cyber researchers this means that they are challenged for searching, developing and verifying methods for recognizing these phenomena. Content analysis is a growing research technique 'for making replicable and valid interferences from texts (or other meaningful matter) to the contexts of their use' (Krippendorff, 2013). This research uses the content analysis technique for the recognizing of the emergent phenomena of the global information networks and cyber operations. The aim is to find out certain principles of the contents of them for focusing the more detailed analysis and forming of simple rules.

A system modeling approach for figuring out the emergent phenomena of a complex system is depicted in Figure 3. The approach assumes that the actors of the complex system are primarily humans and regards social systems as its worldview.

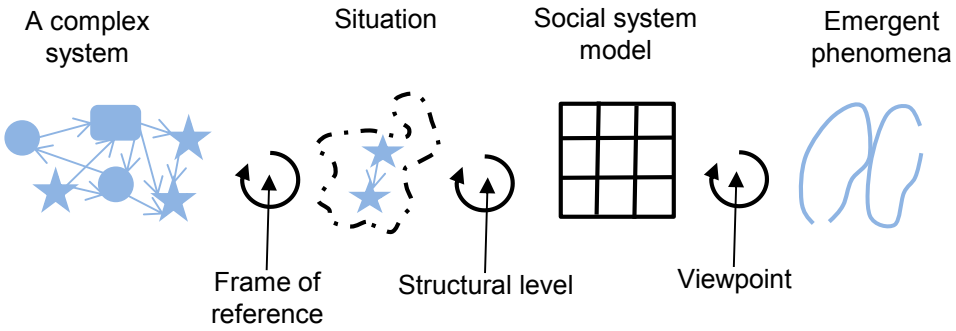

Figure 3. A system modelling approach for figuring out emergent phenomena of a complex system

The system modelling approach begins with information gathering according to the focus of the study, i.e., decision-making situation in concern. The concepts of situation and situation awareness support the identifying of actors and restricting of information flows spatially and temporally. For example, if studies or decisions are to be made about the national cyber strategy vision, the information gathering would cover national cyber strategies published in the other countries, global and local cyber opportunity and threat estimations and cyber-related scientific material as well as anticipated cyber-related infrastructure and product development.

The second part of the approach is the analysis of the contents of the gathered information with the social system model. The analysis with the social system model follows the principle of abstraction. Abstraction is a widely utilized approach in system modelling. It permits dealing with the complexity. The abstraction is performed at the structural level that suits the viewpoint to the contents. The selecting of structural level and viewpoint depend on the situation. For example, if studies are to be made about the national cyber strategy vision, one viewpoint is the international comparison of national cyber strategies. High-level national leader level is a structural level that suits this viewpoint.

Krippendorff (2013) argues that the content analysis is preferable performed with abductive inferences. Deductive and inductive inferences are not considered to be central to content analysis. Abductive inferences are drawn across dissimilar areas, from particulars of one area to particulars of another area (Krippendorff, 2013). The analysis of the contents with the social system model contains classification of the contents into the classes of the social system model. An abductive inference is made with each placing of an item of the contents into one of these classes. Complex systems evolve over time. Therefore, the placing of items into the classes of the social system model is often grouped by time periods, e.g. the sets of results are formed on an annual basis.

The results of system modelling approach are some emergent phenomena of the complex system. The phenomena are identified from a selected point of view. They can be utilized for focusing the more detailed studies. These studies can be implemented by mathematical modelling such as the forming and analyzing of the strategic level metrics or by using some of the basic strategy tools like SWOT analysis. For example, if the adaptation to the current situation seems to be an emergent phenomenon, a SWOT analysis about this

phenomenon can be performed. The aim is that the results of the detailed analysis include simple rules about the complex system. The recognized patterns and formulated rules can be used for understanding and maybe organizing the complexity. For example, a simple rule about the national cyber strategies seems to be that they are derived from the national cultures and priorities. This supports positioning of the cyber strategy implementation activities of nations.

3. CASE STUDIES

3.1 Analysis of a media survey

The aim of the first case study is to identify characteristic and phenomena that need to be known for selecting steps and compositions on the strategic path to cyber society of global information networks. Empirical data consist of public discussions about cyber issues as published in main national newspapers in Finland. The press is considered free in Finland. Finland has succeeded well in several international evaluations concerning the use of information and communication technology and advances in eGovernment such as (Bilbao-Osorio et al., 2014) and (UN, 2012). Emergent phenomena figured out by studying news published in Finland can be considered to include some of the characteristics of global information networks.

The study is a narrow media survey focusing on three sets of news published in Finland in 1994-2014. The news were selected by using "cyber*" as a search criterion. The first set includes news that were published in Aamulehti (1994-2014). The second set contains editorials of Helsingin Sanomat (1994-2014) and the third set contains news classified as science of Helsingin Sanomat (1994-2014). The news were categorized according to the social system model and grouped into two time-basis groups: news published in 1994-2004 and in 2005-2014.

Figure 4 shows a comparison of the news published in 2004-2014 with the news published in 1994-2004. The key to interpret the symbols in Figure 4 are: -X = the change in news is from -5% to -10%, -XX < -10%, 0 = -5% to 5%, X= 5% to 10%, XX > 10%. In the early years in 90s the focus of the news were mainly on culture, i.e., science-fiction movies, stories, music and games. During the following years the focus shifted first to the technology provided to the users and then to information security. Recently security and defence policy level has been included in the general public discussions.

	Interaction is …	*Interaction is externally oriented*		*…internally oriented*
action	**Pattern maintenance**	**Adaptation**	**Goal attainment**	**Integration**
strategic	0	0	x	0
operation art	0	0	0	0
tactic	0	0	0	0
operating	0	0	0	0
structure	**Culture**	**Organization**	**Polity**	**Community**
	-xx	x	xx	0
information	**Values**	**Facts of present**	**Goals**	**Norms**
	0	-xx	x	0
	Initial state		*Goal state*	

Figure 4. Cyber-news published in 2006-2014 compared to cyber-news published in 1994-2004

The major finding is that the cyber discussions have moved from the issues of the initial internal state of a society occurring in the 90s through the initial external state towards the present futures external state as outlined in Figure 5. This flow of the cyber-related public discussions in 1994-2014 is quite similar to information flows described with the social system model. According to information flow thinking the society will next reach the futures internal state. This means that the integration to a cyber-community is likely to happen in the society in the future.

It should be noted, however that the media survey is narrow and addresses only some aspects of evolving society. The recent share of informative cyber-news, i.e. classified as facts of present as well as discussions about the values and norms of cyber have decreased. The focus has shifted to polity and the strategic activities level. This reflects high-level political interest increase in the cyber issues. The technological artefacts of cyber have met the political systems. Examples include political decisions about cyber strategies and critical national and international infrastructure such as the aim to connect Europe and Asia via the Northern Sea Route. The decrease of interest in facts of presents reflects that public already has sufficient information about the features of cyber. Interest has moved to polity which indicates the need to organize and resource the decision-making apparatus and implementation of cyber strategies as prerequisites for efficient and effective cyber defence of society. In addition, cyber capabilities and general resources for performing successful cyber activities need to be developed.

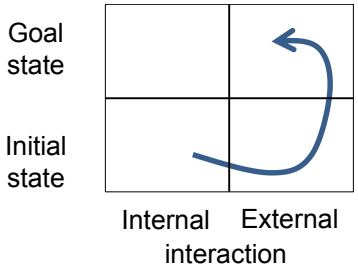

Figure 5. The flow of cyber-related public discussions in Finland in 1994-2014

Next the society will have a need to form norms and interpret the facts of present based on the already published strategic political decisions. The citizens have not yet, however, widely discussed and agreed about the goals and directions of cyber. The raising of international public discussions about the norms and interpretations of the facts of present as well as resourcing and international organizing the forming of norms are needed. This includes forming of general understanding and norms about the required cyber defence capabilities. This is required for guiding the defenders of society to operate in the evolving global information networks on the way that is accepted by the citizens.

3.2 Analysis of workshop findings

The empirical data of the second case study consist of findings of an advanced research workshop held on September 2013 in Geneva, Switzerland (Hathaway, 2014). The aims of the workshop were to exchange expert knowledge and discuss approaches and solutions to cyber defence. The participants of the workshop represented industry, academia and public institutions which have experience with and responsibilities for incident detection and response (Hathaway, 2014). The findings of the workshop were selected for analysis because they were considered to describe well both the current situation and needs for future developments of cyber defence.

The workshop had 21 findings that were categorized according to the social system model. Each finding was not placed on just one category but to all the categories related to it. The results are visualized in Figure 6. The key to interpret the symbols in Figure 6 are: 0< 5%, X = 5-10%, XX > 10%.

	Interaction is …	*Interaction is externally oriented*		*…internally oriented*
action	**Pattern maintenance**	**Adaptation**	**Goal attainment**	**Integration**
strategic	0	0	x	0
operation art	x	0	0	0
tactic	x	0	0	0
operating	x	0	x	0
structure	**Culture**	**Organization**	**Polity**	**Community**
	0	x	0	x
information	**Values**	**Facts of present**	**Goals**	**Norms**
	0	x	x	xx
	Initial state		*Goal state*	

Figure 6. The focus areas of Hathaway's (2014) workshop findings

The analysis of the workshop findings show that in general attention was paid on actions. Structural issues were least discussed. The focus was clearly on norms and pattern maintenance. Facts of present, organization, goal attainment and goals were addressed substantially as well. External initial state issues were discussed less than initial internal or external states' issues. This means that the experienced and competent workshop participants did not favor adaptation to the current situation but norms and pattern maintenance.

Culture and values were not discussed and operational art activities were presented only with pattern maintenance. The discussed operational art activities contain Internet Service Providers and Telecommunication providers to provide upstream security layers stopping the malicious activity before it reaches an organization, national cyber strategies to contain deterrence and defence that adapts to the constantly changing environment, approaching operational problems more holistically with academic and research community and coupling of strategy with market levers to create rewards and punishments, e.g., disruptive regulation to drive insecure products out of the market place.

In the future the discussions about pattern maintenance will influence on addressing of norms. This will raise increasing discussions about the characteristic of cyber community as well as required resources and capabilities. In the future, compositions are needed for forming of joint defence cyber community. In addition, resources for joining this community in affordable and beneficial ways need to be formed.

4. CONCLUSION

The paper outlines and preliminary verifies an approach for figuring out prerequisites which evolving cyber society sets for actors, actions and structures of the defenders of society. The approach allows researchers to outline phenomena of a complex system in a short time and with a small amount of information and few resources. The conducted case studies give an overview on discussions about cyber on society. This overview has been applied for directing research and more detailed information analysis for high-level decision-making. The case studies show that the approach is plausible. More empirical studies are, however, needed to continue the validation of the approach.

When comparing the analysis of public discussions of the first case study to the analysis of professional discussions described as the second case study, it is recognized that the cyber defence professionals discuss more about goals, goal attainment and norms than public. It can be assumed that these professional discussions will in the future raise more public discussions about these topics. Recent observations about global public discussions indicate that discussions about goals and norms are increasing.

The case studies indicate raising discussions about the characteristic of cyber community as well as required resources and capabilities. In the future, compositions are needed for forming of joint defence cyber community. This community will defend society in or through cyberspace. In addition, resources for joining this community in affordable and beneficial ways need to be formed. These are the next steps and future research topics on the strategic path to jointly defended cyber community of global information networks.

REFERENCES

Aamulehti (1994-2014). A Finnish daily published newspaper. Retrieved from the website: www.aamulehti.fi

Ball, P. (2004). *Critical Mass: how one thing leads to another*. London, UK, Sydney, Australia, Auckland, New Zeland: Arrow Books.

Bergson, H. (1911). *Creative Evolution*. University Press of America.

Bilbao-Osorio, B., Dutta, S. & Lanvin, B. (2014). *The Global Information Technology Report 2014, Rewards and Risks of Big Data*. World Economic Forum. Retrieved from the World Economic Forum website: www.weforum.org

Cambridge (2014). *British English Dictionary and Thesaurus, Cambridge Dictionaries Online*. Retrieved from the website: http://dictionary.cambridge.org/dictionary/british/

Habermas, J. (1984). *The theory of communicative action, volume 1: reason and the rationalization of society*. Beacon Press, Boston, MA.

Habermas, J. (1989). *The theory of communicative action, volume 2: lifeworld and system: a critique of functionalist reason*. Beacon Press, Boston, MA.

Hathaway, M. (2014). *Advanced Research Workshop Findings*. In Hathaway, M. (ed.) Best Practices in Computer Network Defence: Incident Detection and Response, IOS Press.

Helsingin Sanomat (1994-2014). Finnish daily published newspaper. Retrieved from the website: www.hs.fi

Holland, J.H. (1996). *Hidden Order: How Adaptation Builds Complexity*. Cambridge, MA, Perseus Books

Kauffman S. (1995). *At Home in the Universe: The Search for the Laws of Self-Organization and Complexity*. Oxford University Press.

Krippendorff, K. (2013). *Content analysis: an introduction to its methodology*, 3rd edition. Sage, Newbury Park, CA, USA

Kuusisto, R. (2004). Aspects on availability. Edita Prima Oy, Helsinki, Finland.

Kuusisto, R., Kuusisto, T. (2009). 'Information security culture as a social system'. In Gupta, M. & Sharman, R. (eds.) *Social and human elements of information security*, pp. 77-97, Information Science Reference, IGI Global, Hershey, New York.

Moffat, J. (2003). *Complexity Theory and Network Centric Warfare*. CCRP, USA.

Parsons, T. (1951). *The Social System*. Free Press, Glencoe, IL.

Piatt, W.E. (1999). *What is Operational Art?* School of Advanced Military Studies, United States Army Command and General Staff, College Fort Leavenworth, Kansas, USA. Retrieved from the website: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA370243

UN (2012). *E-Government Survey 2012, E-Government for the People*. United Nations, Economic & Social Affairs. Viewed on 2 December 2013, < http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf

US ARMY (2010). *Cyberspace Operations Concept Capability Plan 2016-2028*. US ARMY TRADOC Pamphlet 525-7-8, 22.2.2010. Retrieved from the website: https://www.yumpu.com/en/document/view/8916697/cyberspace-operations-concept-capability-plan-2016-2028

US DoD (2013). *JP1-02, Dictionary of Military and Associated Terms 2010*, amended 2013. Retrieved from the website: http://www.dtic.mil/doctrine/dod_dictionary/