Strategic Communication for Cyber-security Leadership[1]

Rauno Kuusisto[1,2,3], Tuija Kuusisto[3,4]

[1]*Finnish Defence Forces Technical Research Center, Riihimäki, Finland*

[2]*Department of Mathematical Information Technology, University of Jyväskylä, Jyväskylä, Finland*

[3]*Department of Tactics and Operations Art, National Defernce University, Helsinki, Finland*
E-mail: rauno.kuusisto@mil.fi; tuija.kuusisto@luukku.com

[4]*Ministry of Finance, Helsinki, Finland*

Abstract: *The purpose of this paper is to form a preliminary hypothesis about how to identify characteristics that a leader needs to focus on when aiming at cyber-security leadership. The paper studies the key concepts and terms of cyber security and presents the physical world and the cyber world framework. The paper refers to a system model of a society and uses that model to analyze the results of two limited media surveys about cyber-related newspaper articles. The media surveys indicate a strong need to organize the cyber world.*

Keywords: *Cyber Security, Cyber-security Theory, Information Security, Governance*

Introduction

Cyber security has gained increasing interest among the management, users, and producers of information systems and e-services. One of the research problems of the cyber world is to identify the issues that a leader needs to focus on when developing cyber-security leaderhip. This paper describes a preunderstanding of phenomena and characteristics that must be considered when studying decision-making systems and strategic communication in the cyber-physical world. The purpose of this paper is to form a preliminary hypothesis about how to identify the characteristics that a leader needs to concentrate on when aiming for cyber-security leadership.

Cyber security or cybersecurity is typically defined as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack". The first known use of 'cyber security' occurred in the year of 1994. (Merriam-Webster 2012) According to von Solms (2010), cyber security is the fifth wave of information security, and its main interest is the security of Internet-based systems. The previous waves (technical, management, institutional, and governance) all exist in parallel with each other (von Solms 2010). On the other hand, cyber-security issues are discussed and actions are taken place on all those waves or levels of organizations. At the technical level, the focus is more on data and

[1] An earlier version of this article was published under the same title in *Proceedings of the 12th European conference on information warfare and security*, eds. R Kuusisto & E Kurkinen, Jyväskylä, Finland, pp. 167- 72.

ISSN 1445-3312 print/ISSN 1445-3347 online

networks and system-security issues such as software vulnerabilities or denial-of-service attacks. At the management level, the interest lies in administrative and policy issues and often cyber strategies. At the institutional and governance levels, organizations are focusing on shared values, norms, and goals as well as good governance practices. A deeper and broader understanding of cyber-security principles is needed for a society to reap the benefits of the digitalization of its vital functions without over controlling or loosening of its cyber security. This balanced cyber security in a society would mean that organizations are able to efficiently and securely perform their tasks with the support of or in the cyber world.

Cyber is defined as "of, relating to, or involving computers or computer networks". Cyber originates from cybernetics. Cybernetics focuses on organizations, patterns, and communication in entities. It is derived from the Greek word '*kybernnētēs*' meaning "pilot, governor" or "to steer, govern" (Merriam-Webster 2012). So, if the basic meaning of cyber is to pilot, steer, or govern, a narrow definition of cyber would be the piloting, steering, and governing of computers and on data networks. A threat is "an expression of intention to inflict evil, injury, or damage" (Merriam-Webster 2012). Following these definitions cyber threats are defined as expressions of intentions to damage the piloting, steering, or governing of computers and on data networks. A broader definition of cyber extends it to the piloting, steering, and governing of systems that are connected by information and communication technology and data networks. Accordingly, cyber threats may be described as expressions of intentions to inflict evil, injury, or damage to systems that are connected by information and communication technology and data networks. These broader definitions allow for the study of vital functions and structures of a society without locking the study with the structural restrictions of any technology.

Based on the broader definition of cyber, the concept of cyber world as presented in **Figure 1** 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 makes it possible to deal with the essential issues and phenomena that emerge from this novel domain. Those issues include human social behavior supported by information-technology solutions. Information technology is set as a position of enabler rather than a dominator of the human existence.

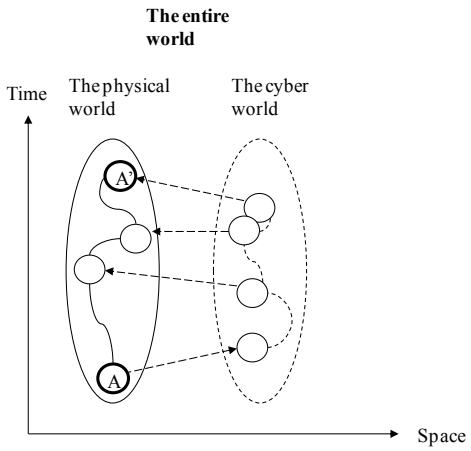

Figure 1: The interaction between the physical world and the cyber world.

Leadership is a popular term typically defined as "the office or position of a leader". Other definitions of leadership include the "capacity to lead" or "the act or an instance of leading".

One of the definitions of leading is "providing direction or guidance" (Merriam-Webster 2012). So, from an action point of view, cyber-security leadership is defined as providing direction or guidance for cyber-security activities. In addition, according to the presented definitions, cyber-security leadership also has to include the capacity to lead, and the capacity to lead has to cover activities on the technical, management, institutional, and governance levels of a society or an organization.

Some of the definitions of the term strategic communication include the "purposeful use of communication by an organization to fulfill its mission" (Hallahan et al. 2007) and, in a nation-specific context, "focused United States Government efforts to understand and engage key audiences to create, strengthen, or preserve conditions favourable for the advancement of United States Government interests, policies, and objectives through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all instruments of national power" (DOD 2012). Strategic communication has its roots in various information warfare approaches. It includes collaborating and participating encouraging activities to communication and the use of the modern technology such as social media in cyber world. The concepts of strategic communication and cyber security are connected in several ways. From the cyber-security point of view, communication (including strategic communication) is considered an enabler of cyber security. Cyber-security leadership includes the collecting and distributing of effective information about cyber-security situations, resources, means, and goals. In addition, strategic communication supports cyber security in the long term by actively refining the shared values and norms of a society or an organization. On the other hand, cyber security is needed for strategic communication to reach its goals with the support of and in the cyber world.

In the cyber world, communication (including the strategic communication between organizations and individuals) is different than it is in the physical world, because the cyber world does not support all senses. The most important missing sense is touching, and its absence changes the way communication is accomplished. The missing power could be compensated for in various ways. These ways may transform methods of self-expression in the physical world as well. There is a great deal of information in the cyber world that is essential for the functionality of the cyber world itself, but which does not reveal itself to the users of the cyber world. There are archives of essential information about and for individuals and organizations in the cyber world. The physical location of those archives is not necessarily kept in good control or even known by users. Likewise, the duration of archiving information is not necessarily user-controlled. Such information that is nonrecurring, thus vanishing forever after expressed in the physical world, may be archived in the cyber world. This may have consequences for the way of humans will act in the futures.

Information in both the cyber and the physical world is vulnerable to various security threats. As an endlessly expanding domain, the cyber world offers splendid opportunities for misuse of information. There are new kinds of structures and activities manifesting in novel ways in the the cyber world that are waiting for relevant and acceptable regulations that do not yet exist. Regulations and norms form a complex system. Some norms are acceptable and good from one person's point of view, but vain or even disastrous for someone else. Interpretation of norms and their value vary for several reasons. The cyber world is more or less open. Information travels at the speed of light, and borders are in different places than in the the physical world.

The Physical-world and the Cyber-world Framework

Outlining a physical- and cyber-world framework increases comprehension of the required leadership in the cyber context. The framework is derived from research on organizations and information technology. The framework consists of two dimensions: the physical world and the cyber world as presented in **Figure 2**. The framework models activities that are executed in either the physical or cyber world. For example, traveling by a car is an activity that is executed and occurs in the physical world. If the driver needs a map update for his or her navigation system and pays for the map by a credit card, he or she would be performing an activity that is executed in the physical world but occurs in the cyber world. The purchased map's updating to the navigation system would be an activity that is executed and occurs in the cyber world. The driver receiving route instructions is an activity executed in the cyber world and occurring in the physical world.

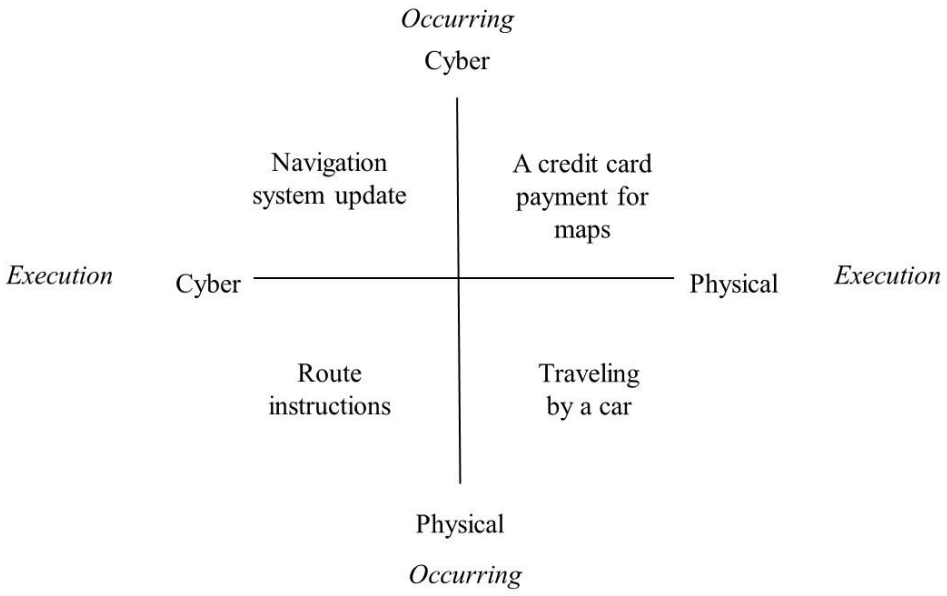

Figure 2: The physical-world and the cyber-world framework.

An example that illustrates the interaction within the physical- and cyber-world framework within the context of cyber security is the explosion of a datacenter. The explosion is an activity executed in physical world and occurring in the cyber world. A typical denial-of-service attack, however, is executed and occurs in the cyber world. Recently, activities executed in the cyber world and occurring in the physical world have garnered a great deal of interest. For example, malware on manufacturing systems or controlling systems can have an effect on the integrity of the system's information. The impact of the executed activities can be outlined as the modified information causes unpredictable behavior of the physical components of the manufacturing systems.

A System Model of a Society

All systems as well as social systems can be considered as information-driven activity cycles in a structure. This very early discovered feature (Aristotle) says that systems consist of a structure, actions, and information. They will produce activity, when the right kind of information is fed into their structures. The produced activity will act as input information for the systems to produce more activity. Habermas (1984, 1989) combines theories of the social sciences and system thinking. He states that a social system contains time and space dimensions. It has an initial state and a goal state. The system's communication orientation is

both internal and external. Habermas (1989) refers to Talcott Parsons' (1951) thinking that information directing activities of an actor contains four basic classes: values, norms, goals, and external facts. The actor is, for example, a state, an organisation, a team, or even an individual. In the information-refining process of an actor, the values have effects on the norms; the values and the norms both have effects on the goals; and all those classes have effects on the exploiting of external facts. Activities using external facts to change values are adaptation, goal attainment, integration, and pattern maintenance functions. The structural phenomena of social systems contain culture, community, polity, and institutions. Cultural systems are more solid than communities, which are again more solid than polity structures and institutions (Habermas 1989). Information fed into a structure produces various actions based on information categories. Values influence on the ways to act and maintaining patterns. Norms urge forward the integration into the community. Goals guide the reach toward objects, and external facts produce adaptation to the requirements of the surroundings.

Facts of present, including means and resources are used for putting such an activity in practice, which will lead the actor to fulfil its goals as optimally as possible. Originally in Habermas' theory, the user of resources, that is, the institution is economy. However, the concept of a resource-using structure can be applied to other entities. For example, marketing, production, or research and development departments are potential resource-using structures in an enterprise. (Kuusisto 2004) Cyber security and strategic communication are potential resource-using structures in a society and in an organization. The leadership aspect of cyber security considers cyber security a resource-using structure. Cyber-security leadership is required to reach the goals of a society or an enterprise, that is, to secure the units and vital functions of a society. Leadership especially needs strategic communication as a means to provide and deliver information for directing the resources of the cyber security.

A general model that contains the aspects of the social system described in the previous paragraphs appears in **Figure 3**. This model is derived from a more detailed figure of organization dynamics presented in 'Information security culture as a social system' (Kuusisto & Kuusisto 2009). Each field contains a certain kind of action, structure, and information. The time dimension contains initial state and future state, and the space dimension contains internal interaction and external interaction. Interactivity relationships exist between a field and the fields above or below that field. In addition, interaction exists across neighbouring action and information fields. 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 from different functional parts of the system is a combination of the influence of neighbouring parts of the system and the external input of each subsystem of the comprehensive system. It can be easily recognized that this kind of system is complex and, thus, emergent.

	Interaction is…	*Interaction is externally oriented*		*…Internally oriented*
action	Pattern maintenance	Adaptation	Goal attainment	Integration
structure	Culture	Organization	Polity	Community
information	Values	Facts of present	Goals	Norms
	Initial state		**Goal state**	

Figure 3: A system model of a society

People are acting in the structures of a social system guided by the structure itself and obeying more or less the internal norms. The people acting in a social system are producing information both inside the system and between other, neighbouring systems. This kind of information flow and the continuous emergence of new kinds of interpretations form a complex system that may be difficult to figure out and is practically impossible to control. However, the model can help to create understanding about the complex nature of the ever-interacting and dynamically-evolving system of various subparts as well as the phenomena of the comprehensive system; that understanding can lead to the development of relevant enough acts that make it more convenient to live in this kind of new surroundings.

A Media Survey on Cyber-related Newspaper Articles

The first author of this paper conducted limited media surveys on the cyber-related newspaper articles in the autumn of 2011 and 2012. He collected cyber-related news published between 6 September and 17 November in 2011 and between 7 August and 15 November in 2012. The news was published mostly in one of the main newspapers in Finland, *Helsingin Sanomat* (2011 & 2012). The number of articles collected was 83 in 2011 and 136 in 2012. As a part of their own studies, two groups of graduate students categorized the news according to the model described in **Figure 3**. The first author of this paper then conducted a content analysis of the categorized news according to Krippendorff's (1980) method. The results of the analysis are presented in **Tables 1** and **2**.

	Interaction is…	*Interaction is externally oriented*		*…Internally oriented*
action	**Pattern maintenance**	**Adaptation**	**Goal attainment**	**Integration**
	16	17	20	4
structure	**Culture**	**Organization**	**Polity**	**Community**
	7	0	6	3
information	**Values**	**Facts of present**	**Goals**	**Norms**
	9	10	7	1
	Initial state		**Goal state**	

Table 1: Reported cyber-related news (%) in one main newspaper in Finland in autumn 2011

	Interaction is…	*Interaction is externally oriented*		*…Internally oriented*
action	**Pattern maintenance**	**Adaptation**	**Goal attainment**	**Integration**
	13	13	9	3
structure	**Culture**	**Organization**	**Polity**	**Community**
	7	5	6	3
information	**Values**	**Facts of present**	**Goals**	**Norms**
	10	17	5	8
	Initial state		**Goal state**	

Table 2: Reported cyber-related news (%) in one main newspaper in Finland in autumn 2012

The media surveys showed that the cyber-physical worlds modelled in **Figure 2** are discussed in public. The key findings of the first media survey include that the organization structures were not discussed. This means that it was not known or a matter of general interest what the responsibilities were and who was responsible for 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 showed that the internal discussions in society about the norms and rules of cyber activities and behavior have begun. In addition, the survey confirmed that external discussions in society about the facts of cyber activities and organization had increased (compared to the results in 2011). This means that people want to know what kind of norms will guide the world and how this cyber-physical world will be perceived in the future. A strong need to organize the cyber world seems to be imminent. However, the ways to integrate the various communities are still unclear. This means that the basic question is whom we want to lead us. On the other hand, it should be noted that the presented results of the media surveys are one interpretation about the current status of cyber world in a society.

The key findings of the media surveys show that in the current cyber-era the structures of the changing world are unclear; the future does not reveal understandable patterns; and the future is undetermined and open. Activities perceived from the world are changing, and cultural changes have an effect on maintaining activity patterns. The decision-making apparatus is changing, and goals reveal themselves in a different way than before and seem not to be under any control. It is not necessarily clear and well enough known which are the mutually understood norms and what is and will be the safe community to belong to and which other communities are the ones to integrate with. The future of ‘me’ is uncertain because the concept of ‘us’ is tottering. Adaptation to the new situation takes place under the control of somebody else. The general feeling is that the future will be reached in an uncontrolled way.

Conclusions

This paper presents concepts, models, and the results of media surveys regarding the increasing understanding of those phenomena that may be important when studying the complexity of cyber security. The media surveys show that the proposed models presented in **Figures 2** and **3** are plausible for studying issues that a leader needs to communicate when developing cyber-security leaderhips. In addition, the media surveys point out that the focus of discussion about the cyber-physical world in a society is changing over time. This means that a leader needs to change his or her strategic communication profile to be able to effectively lead and develop cyber security. Continuous collecting of empirical data is required for the optimizing of strategic communication. On the other hand, wider and deeper sets of empirical data are needed to verify and validate the models and conclusions based on the models.

What is certain is that there is a need for cyber-security leadership. This means providing directions and guidance for cyber-security activities in the comprehensive cyber-physical world. Strategic communication serves as a means to provide and deliver information for the planning and directing of the resources of cyber security.

References

DOD 2012. *DOD dictionary of military terms*, viewed 19 December 2012, <http://www.dtic.mil/doctrine/dod_dictionary/>.

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

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

Hallahan, K, Holtzhausen, D, van Ruler, B, Verčič, D & Sriramesh, K 2007, 'Defining strategic communication', *International Journal of Strategic Communication*, vol. 1, no. 1, pp 3-35.

Krippendorff, K 1980, *Content analysis: an introduction to its methodology*, Sage, Newbury Park, CA.

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

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

Merriam-Webster 2012, *Merriam-Webster online dictionary*, viewed 17 December 2012, <http://www.merriam-webster.com>.

Parsons, T 1951, *The social system*, Free Press, Glencoe, IL.

von Solms SHB 2010, 'The 5 waves of information security – from Kristian Beckman to the present', *SEC2010, IFIP Advances in information and communication technology*, eds. K Rannenberg, V Varadhajaran & C Weber, vol. 330, pp. 1-8.