The Open Definition of Cyber:
Technology or a Social Construction?

Martti Lehto, Finnish National Defence University, Finland

Aki-Mauri Huhtinen, Finnish National Defence University, Finland

Saara Jantunen, Finnish National Defence University, Finland

ABSTRACT

Security strategy work requires a definition for 'cyberspace'. This article discusses national definitions and analyses their contents. Defining what cyberspace is equals the exercise of political power. Therefore, it is important to discuss what the definitions mean in practice - whether cyberspace is seen as a restricted mathematical-technological domain or a social construction. Government publications highlight the technological aspect of cyberspace, whereas threats stem from human behaviour. For some, cyberspace is a primary operational environment for national security that must be protected with defensive and offensive military means. For others, cyberspace is primarily a digital civil society in which the free flow and usability of information and the identity and anonymity of citizens must be secured. Cyberspace can also be seen as a place for business, where material and immaterial products and services can be offered. The authors argue for the broad definition of cyberspace, incorporating both technological and social concepts. But cyberspace may never be comprehensively defined. If only a strictly technology-oriented approach is used to define cyberspace, many of its risks and problems cannot be addressed. Cyberspace allows the exercise of power; therefore, its definition should not be reduced to pure technology.

Keywords: *Cyber Strategy, Cyber Warfare, Cyberspace, Security, Strategic Planning*

INTRODUCTION

The main argument in this paper is that the organizational development of the military follows the development pattern of the military-industrial complex: economic steering surpasses the political Clausewitzian steering and the 'de-territorialization' of the Comprehensive Approach planning model centralizes the traditional Services (Army, Navy, Air Force) into common (virtual) capabilities. Deep down it is about power struggle within the armed forces. This is visible in, for example, Afghanistan and the working environment frustrations of the Joint Force Command Headquarters. At the same time economic steering is creating an unending network of 24/7 're-territorialization', mostly in the cyber defense domain, where defense economic resources will be moved to. The traditional bureaucracy of a military organization is replaced by the 'marketization' of the military culture. Increased outsourcing partnerships and the increased influence of third sector actors in the battle space are examples of

DOI: 10.4018/ijcwt.2011040101

this marketization, as well as the transformation of the politico-military strategic level from conducting international politics or diplomacy to a level with strategic communication, reputation management and increased information operations.

Especially small European states, such as Finland, are in a challenging situation in terms of their national identity. They have to ask themselves whether they should accept the geopolitical change and the new situation caused by the emergence of the cyber dimension into the security functions in society. This has transformed the citizens' and, consequently, the politicians' image of a threat from a large-scale war to 'humanitarian' operations conducted far from Europe. The compartmentalizing of the new threats into the computer and Internet world also moves war and violence behind the curtain of clean and hygienic technology. We do not think that a computer might be as destructive as a nuclear weapon or a missile. We don't even dare to think what a large-scale cyber war would be on a global level: most likely something much worse than nuclear war. Our identities and everyday lives are totally dependent on information technology. The worst post-modern dream could be the virtual (invisible) rhizome or a network of nuclear weapons and computers that would quickly change our ideas of far-away asymmetric wars into something that is a total and global cyber war. The worst possible world is a typical concept for the post-modern thinking. The only way to protect oneself from this kind of thinking is to allow participative thinking for everyone. Therefore, all central information systems involved with national security should be open source and allow everyone to participate and observe. In its own way, the Wikileaks principle was attempting to achieve this.

Out of the Real Security Box

Why is the myth of security simplified into the concept of gap? Because we can no longer control the network of old classical and rational tools. The cyber domain is the space that everyone needs but no one can control. There is no longer a balance between subject and object. We have to constantly move to understand our environment. There is no longer a military hill for commanders.

First, we try to achieve the convergence situation. An overall aim in society is to increase the connectivity and capability for communication and dynamics of technological systems - for the reasons of effectiveness and functionality. On the other hand, economic factors demand large scale savings, and these are expected to be brought by centralization. These aims are best reached if the systems adhere to the same standards in their communication, and use very similar modules in their operations (hardware and software components). This is followed by the so-called "all the eggs in one basket" phenomenon: also vulnerabilities can be more extensively taken advantage of, and due to differences in the mending process, they can also be taken advantage of for a longer period of time.

Second, we believe in integration. For reasons of effectiveness and economy, systems should "outsource" some of their tasks to systems that are more specialized and optimized for those tasks. The bottleneck in this type of outsourcing is often the data transfer needed for setting new tasks and gaining answers, which again results in better connectivity. The tightening of connectivity is followed by even tighter integration, and "outsourcing" by a greater inter-dependency. This forms a threat because the entity is not protected to the same extent. Even in sensitive systems vulnerabilities can be found "through the kitchen".

Third, we are moving from material infrastructure to virtual infrastructure. The concept of infrastructure is extending into cyberspace, as systems become more and more interdependent and support each other. If there are enough systems that can be utilized, the system providing the service can be considered as their infrastructure. It is easier to maintain the infrastructure, update it and move it away from a crisis area. Networking this type of infrastructure also makes it more durable from the point of view of accessibility. The infrastructure

can form a threat in that, as an application, it also becomes a channel for attack for methods functioning through the cyberspace, and on the other hand, the effects of this can also progress through the network.

The geopolitics of the physical real world intertwine with the cyber world. Cyberspace and the physical world are more and more difficult to handle and model separately. The importance of the physical world for cyberspace is clear (e.g., the dependency of the cyber world on electricity or physical processors), but the development in the opposite direction is also rapid. The most quoted example of this is Stuxnet, but there is another phenomenon that links cyberspace all the more closely as an effector of the physical world: rapid production (e.g., 3D printers). The areas of use of 3D printing are being significantly extended: research is being done in, e.g., bioprinting (producing human organs) and in building technology. The principle of rapid production leads to the products being located only in cyberspace for a longer time, until they are transferred to the physical world close to the target. This also means that the vulnerabilities of cyberspace are very widely derivable to the physical world.

The possibilities for communication grow rapidly in cyberspace. There are hardly any possibilities for limiting communication. Theories and solutions for encryption that focus on data content already exist for confidentiality and the integrity of content and can inevitably be expected to be required in cloud services. It is probable that such virtual separate networks will be created for different sensitive purposes, where the principle is that the service is available only in a very controlled environment. However, such separate networks cannot be networks that are of public utility or have an extensive purpose.

The Comprehensive Approach planning requires continuous self-control from the actors as well as the regulation and management of the various information networks and strains. Therefore the bureaucracy of a military organization is no longer based on positional authorities, but on self-regulatory mechanisms that are utilized in the economic markets and installed in individual soldiers. Those military leaders who are too set in their ways to adapt to new operation procedures will be replaced either by technology or by civilian experts, whose status will never rival that of the officers.

Why Do We Need the Comprehensive Approach?

We have to plan and prepare for the simultaneous occurrence of multiple crises or catastrophes. One also needs to consider how the effects of multiple crises can reinforce one another so that the overall result is worse than if merely one occurred by itself. The fact that this process is complex, uncertain, and never perfect is not an excuse for doing nothing (Alpaslan & Mitroff, 2010, p. xvi).

In other words, none of the components that constitute a problem can be taken apart and analyzed independently from all the other problems that contribute to it - a mess. A mess is a complex system of problems. For instance, the 'military problem', or better yet the 'military mess', exists alongside with other messes such as crime, health care, poverty, real estate values, etc. The concept of a mess is essentially synonymous to the concept of a 'system'. In fact, there is no such thing as a single crisis that is not embedded in a system of other crises. All crises are messes, but all messes are not crises (Alpaslan & Mitroff, 2010, p. xiv).

All crises are human-caused. The spread of individual risk also increases systematic risk. The root problem is what has been termed "rational irrationality" – behavior that, on the individual level, is perfectly reasonable but that, when aggregated in a complex system, produces calamity (Alpaslan & Mitroff, 2010, p. xvii).

Problems have more than one solution because they have more than one formulation. The concept of problems has a different content than the concept of exercises. The solutions not only contribute to the problems, but they actually make them worse (Alpaslan & Mitroff, 2010, p. 20). Typically, the war in some special area has made this area less stable. Problems are

Table 1. Theoretically analyzing security (adapted from Alpaslan & Mitroff, 2010, pp. 11-12, 22)

Parts	Analytical	Technical	Whole
- Our technology is reliable and it will protect us	- Details, Facts, Formulas, "here and now", number of deaths, injuries, financial cost, collapse of companies - independent causes and effects, efficient means problems	- The big picture, system, systemic costs, collapse of industries - a system of ill-defined, fuzzy, messy, ethical means and ends problems	-Our systems are reliable and will protect us"
- My immediate work group, family, and I are good, and will not betray or harm anyone	- Specific individuals, stories, feelings, values, emotional cost, collapse of personal assumptions - existential problems (efficient means problems: there is something wrong with me)	- Societal values, politics, societal costs - a system of wicked, fuzzy, messy (ethical means and ends problems: there is something wrong with us)	- My country, community, company, and industry are good and will not betray or harm us"
Personal	Analytical	Technical	People

inherently "messy". Take away the messiness and you take away what makes them problems. At the same time you not only make problems worse, but make the solutions more difficult. Problems do not exist independently of the mess in which they are embedded (Alpaslan & Mitroff, 2010, p. 20).

"To 'resolve' a problem means to contain it within acceptable limits" (Alpaslan & Mitroff, 2010, p. 25). It means accepting that problems, such as terrorism, are not wars that can be won, but social diseases or pathologies that can only be managed as best as we can over time.

According to Hutton (2010, p. 111), the key to capitalist dynamism was to bring together risk-taking finance with risk-taking entrepreneurs to introduce new innovations. We need the so-called creative destruction, in which existing elites stand to lose a lot, possibly everything, from creative destruction. They will resist change to the last. Creative destruction had an inherent bias to productive entrepreneurship.

There are two fundamental attributes of networks that determine their resilience or fragility. The first is that they are always much more networked and interconnected than anyone assumes. The degrees of separation between individuals in large universes are surprisingly small. The lack of awareness about interconnectedness had plagued the financial system for years – both regulators and participants. The second characteristic of networks is that a small minority of nodes have an enormous number of connections, while the majority has just a few. In social life we understand this as the rich getting richer and the poor getting poorer (Hutton, 2010, pp. 200-201).

In system thinking, the physical science, certainly knowledge about the physical world, are inseparable from the social sciences and knowledge about the social world (Tables 1 and 2) (Alpaslan & Mitroff, 2010, p. 118).

The Definition of Comprehensive Approach

The essential foundation for the Comprehensive Approach is the willingness of individuals, units, departments and organisations to collaborate with others (Johnson, 2010; LTC, Simon Maj, & Duzenli, 2012; Rintakoski et al., 2008). In the spirit of the military-industrial-complex civilian organisations have their own plans and agendas and do not necessarily have the resources or will to help in the military planning process, unless they can benefit from the process. There has to be incentives for civilian organisations to participate. Knowledge development is the

Table 2. The difference between technical and psychological aspects of security (adapted from Alpaslan & Mitroff, 2010, pp. 134, 154)

Parts/Components	Technical	Scientific	Whole/Systems
Risk is an objective, quantifiable, measurable, real phenomenon.	Harry Markowitz (risk as co-variation, volatility) James Burke (risk as probability of loss)	Charles Perrow (interactive complexity, normal accident) Ulrich Beck (manufactured risk)	Risk is designed into and produced by technologies
Risk is a subjective phenomenon.	Daniel Kahneman and Amos Tversky (cognitive biases)) Paul Slovic (perceived risk)	Mary Douglas (risk and culture) Karl Weick (organizational sense making)	Risk is embedded in social and cultural belief systems.
Personal/Individuals	Psychological	Moral	People/Collectives

key to improving one's understanding of the environment and one's own role in it is to make this frame of intentionality explicit. This means analyzing what influences the perception of a certain situation. This kind of thinking takes us from "need-to-know" to "need-to-share" thinking.

NATO and western armed forces have long been seeking a solution for controlling the powers of crises such as the ones in Afghanistan and Iraq. Pure military power seems to be ruled out since kinetic weapons cannot be used to create local trust and democracy. The elimination of individual dictators and their governments has not led to a democratization policy among citizens. The challenge faced by military operations has been fitting them into the political process.

CA planning requires continuous self-control from the actors as well as the regulation and management of the various information networks and strains. Therefore, the bureaucracy of a military organization is no longer based on positional authorities but on self-regulatory mechanisms that are utilized in the economic markets and installed in individual soldiers. Those military leaders who are too set in their ways to adapt to new operational procedures will be replaced either by technology or by civilian experts whose status will never rival that of the officers. Also we need new kinds of concepts or metaphors to explain this self-control of military actors.

The core questions of the assessment are whether the operations are progressing according to plan and whether they have the anticipated outcomes, and if not, what needs to be adjusted. Traditionally these questions have been addressed by reports through the chain of command and these reports have usually been of a qualitative nature and based on subordinate commanders skill and experience. In NATO and especially in the US the culture has been that of quantitative measures. With evidence based quantitative methods there is an abundance of data but there have been great difficulties linking the data to the goals and objectives. The old saying that everything that counts cannot be counted and everything that is counted and does not count still holds true. The question is to find a balance between experience based (leadership) and evidence based (management) methodology.

Cyber Security in Cyberspace

Within the last few years several countries have formed their cyber security strategies, by which they aim to respond to the challenges that various threats in the cyber world cause. Finland is forming its own cyber security strategy and it will be completed in 2012.

In their cyber strategies countries define cyberspace in different ways. The definition describes their perception of the nature of cyberspace. According to the Canadian cyber

strategy: "Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks" (Public Safety Canada, 2010, p. 2).

In the cyber strategy of Germany: "Cyberspace includes all information infrastructures accessible via the Internet beyond all territorial boundaries and cyberspace is the virtual space of all IT systems linked at data level on a global scale." In Germany all players of social and economic life use the possibilities provided by cyberspace. As part of an increasingly interconnected world, the state, critical infrastructures, businesses and citizens in Germany depend on the reliable functioning of information and communication technology and the Internet (Federal Ministry of the Interior, 2011, pp. 2, 14).

Definition of cyberspace according to the United Kingdom is: "Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information." It includes the internet, but also the other information systems that support businesses, infrastructure and services. Digital networks already underpin the supply of electricity and water to homes, help organize the delivery of food and other goods to shops, and act as an essential tool for businesses across the UK ("The UK Cyber Security Strategy," 2011, p. 11).

In the United States' cyber strategy says, that "cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security" (National Strategy to Secure Cyberspace, 2003, p. vii).

Thus, the healthy functioning of cyberspace is essential to US economy and national security. Most critical infrastructures, and the cyberspace on which they rely, are privately owned and operated in US. The technologies that create and support cyberspace evolve rapidly from private sector and academic innovation" (Bush, 2003, pp. 1-2).

The goals in the cyber strategy also describe how the country sees the cyber world.

The aim of the Australian Government's cyber security policy is: "maintenance of a secure, resilient and trusted electronic operating environment that supports Australia's national security and maximizes the benefits of the digital economy. The Australian Government defines cyber security as: "relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means" (Commonwealth of Australia, 2009, p. 5).

In Canada "success in cyberspace is one of our greatest national assets. Protecting this success means protecting our cyber systems against malicious misuse and other destructive attacks" (Public Safety Canada, 2010, pp. 2-3, 8):

- Reflects Canadian values such as the rule of law, accountability and privacy;
- Allows continual improvements to be made to meet emerging threats;
- Integrates activity across the Government of Canada;
- Emphasizes partnerships with Canadians, provinces, territories, business and academe; and
- Builds upon our close working relationships with our allies.

In Estonia "the National cyber security is a broad term encompassing many aspects of electronic information, data, and media services that affect a country's interests and wellbeing." Toward this end, the most important policy domains include reducing the vulnerability of cyberspace, preventing cyber-attacks in the first instance and, in the event of an attack, ensuring a swift recovery of the functioning of information systems (Ministry of Defence, 2008, p. 7).

In The Netherlands "cyber security is freedom from danger or damage due to the disruption, breakdown, or misuse of ICT." The Strategy's goal "is to strengthen the security of digital society in order to give individuals, businesses, and public bodies more confidence in the use of ICT". To this end, the responsible public bodies of the Netherlands will work more effectively with other parties to ensure the

safety and reliability of an open and free digital society. This will stimulate the economy and increase prosperity and well-being. It will ensure legal protection in the digital domain, prevent social disruption, and lead to appropriate action if things go wrong (ENISA, 2011, pp. 4-5, 7).

In Germany "the availability of cyberspace and the integrity, authenticity and confidentiality of data in cyberspace have become vital questions of the 21st century. Ensuring cyber security has thus turned into a central challenge for the state, business and society both at national and international level" (Federal Ministry of the Interior, 2011, p. 2).

The vision for the United Kingdom is "in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society" ("The UK Cyber Security Strategy Protecting," 2011, p. 21).

In the United States the purpose of the cyber security strategy "is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact." Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from the entire society of the US —the federal government, state and local governments, the private sector, and the American people (National Strategy to Secure Cyberspace, 2003, p. vii).

In the United States the information technology revolution has changed the way business is transacted, government operates, and national defense is conducted. These three functions now depend on an interdependent network of critical information infrastructures that the USA refers to as cyberspace. It is the policy of the United States to prevent or minimize disruptions to critical information infrastructures and thereby protect the people, the economy, the essential human and government services, and the national security of the United States (National Strategy to Secure Cyberspace, 2003, p. 13).

The cyberspace environment of the United States rewards innovation and empowers individuals; it connects individuals and strengthens communities; it builds better governments and expands accountability; it safeguards fundamental freedoms and enhances personal privacy; it builds understanding, clarifies norms of behavior, and enhances national and international security (Obama, 2011, p. 8).

The United States "will work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation." To achieve that goal, the United States will build and sustain an environment in which norms of responsible behavior guide states' actions, sustain partnerships, and support the rule of law in cyberspace (Obama, 2011).

These examples show that cyberspace has a different meaning in different countries. Nations have chosen different perspectives for their cyber strategies. These alternatives are focused either on the public sector, on the private sector (industry and business) or on civic society. In every strategy we may identify all three focuses but priorities are different. The public sector emphasizes the role of the government to manage cyber security and cyber defence. The cyberspace environment of the public sector is the national critical infrastructure (CIP) and critical information infrastructure (CII). Many nations also emphasize the importance of the availability, confidentiality and integrity of information.

In the private sector safe and reliable ICT is essential for the prosperity and well-being of the nation, and it serves as a catalyst for further sustainable economic growth. The digital economy is the global network of economic and social activities that are enabled by platforms such as the Internet, mobile and sensor networks. A successful digital economy is essential for the economic growth and ability of the nation to maintain international cooperation. The digital economy is highly dynamic. It will ultimately encompass the entire economy and many, if not all, aspects of society.

Infrastructure protection requires more security with regard to IT systems used by citizens. Users need appropriate and consistent information concerning the risks related to the use of cyberspace systems and on security measures they can take to use cyberspace in a secure manner. Citizens want their privacy, identities and physical wellbeing protected from cyber predators. The civic society focus means that the ultimate goal is to create a culture of cyber security whereby citizens are aware of both the threats and the measures they can take to ensure the safe use of cyberspace.

CONCLUSION

Digital cyberspace is global. Cyber-attacks and disruptions instantaneously transcend national borders, cultures, and legal systems. Nothing cyber can be discussed in a purely technological context. The social aspect of cyberspace must be recognized not only in strategy work, but in the practices and processes of acting it out. Cyberspace should not be reduced to a tool in terms of its function, as all things that exist in the physical world, have or will have their digital reflection in the virtual world. Judging by the definitions, cyberspace should ideally be reliable and confidential, and most definitions characterize it as a mere information sharing tool. This positions it in the context of government responsibility and restriction. However, cyberspace cannot be guarded more strictly than physical society without impacting its socially significant use and functions negatively. It should be accepted that its complexity cannot be reduced.

The Comprehensive Approach model (CA) illustrates the professional community, whose self-control tolerates opening its own activities to include external actors. Actually, the myth means that security is built together with the opponent. The motto "know your enemy" has changed into "communicate with your opponent". Because the operational environment of the struggle is cyberspace, the form of combat is communication. People are the center of gravity. We combat among people. The bullets are replaced by words, concepts and pictures. The target is not only certain individuals, but whole networks. Publicity makes communication continuous and open. The border between attack and defense disappears along with the boundary between what is public or private. A good example of this is Wikileaks or the defense of an open source code.

REFERENCES

Alpaslan, C. M., & Mitroff, I. I. (2011). *Swans, swine, and swindlers. Coping with the growing threat of mega-crises and mega-messes*. Stanford, CA: Stanford University Press.

Armistead, L. (2010). *Information operations matters. Best practices*. Washington, DC: Potomac Books.

Bush, G. (2003). *The national strategy to secure cyberspace*. Retrieved from http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

Commonwealth of Australia. (2009). *Cyber security strategy.* Retrieved from http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(4CA02151F94FFB778ADAEC2E6EA8653D)~AG+Cyber+Security+Strategy+-+for+website.pdf/$file/AG+Cyber+Security+Strategy+-+for+website.pdf

ENISA. (2011). *National Cyber Security Strategy (NCSS): Success through cooperation*. Retrieved from http://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011

Federal Ministry of the Interior. (2011). *Cyber security strategy for Germany*. Retrieved from http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

Hadnagy, C. (2011). *Social engineering. The art of human hacking*. Indianapolis, IN: Wiley.

Hutton, W. (2010). *Them and us. Changing Britain – Why we need a fair society*. London, UK: Little, Brown.

Johnson, T. F. (2010). The comprehensive approach and the term of "EBAO". *The Three Swords Magazine*, 10-13. Retrieved from http://www.jwc.nato.int/files/17_10_Magazine.pdf

LTC, Simon Maj, G., & Duzenli, M. (2012). The comprehensive operations planning directive. *NRDC-ITA Magazine, 14*. Retrieved from http://www.nato.int/nrdc-it/magazine/2009/0914/0914g.pdf

Ministry of Defence. (2008). *Cyber security strategy*. Retrieved from http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf

Obama, B. (2011). *International strategy for cyberspace: Prosperity, security, and openness in a networked world*. Retrieved from http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Public Safety Canada. (2010). *Canada's cyber security strategy - For a stronger and more prosperous Canada*. Ottawa, ON, Canada: Author.

Reich, J. W., Zautra, A. J., & Hall, J. S. (Eds.). (2010). *Handbook of adult resilience*. New York, NY: The Guilford Press.

Rintakoski, K., & Autti, M. (Eds.). (2008). *Comprehensive approach. Trends, challenges and possibilities for cooperation in crisis prevention and management*. Helsinki, Finland: Edita Prima.

The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. (2011). *Cabinet Office*. Retrieved from http://www.carlisle.army.mil/dime/documents/UK%20Cyber%20Security%20Strategy.pdf

Martti Lehto, Researcher, COL (ret.), is working as a part time researcher at the University of Jyväskylä in the Department of Mathematical Information Technology of Faculty of Information Technology. His research area is cyber defence and cyber security in public and private environments. He is also finalizing his dissertation at the Finnish National Defence University. The theme is the Finnish Air Force C4ISR System Evolution from the perspective of Air Power Theory, National Institutions and Foreign C4ISR Development. He is also the Editor-in-Chief for the Military Magazine *(Sotilasaikakauslehti).*

Aki-Mauri Huhtinen, PhD, Professor, LTC (G.S.), is Docent of Practical Philosophy at the University of Helsinki and Docent of Social Consequences of Media and Information Technology at the University of Lapland. The author is also Docent of Information Security and Information Operations at the University of Technology in Tampere. Huhtinen works in the Department of Leadership and Military Pedagogy at the Finnish National Defence University.

Saara Jantunen has studied English language and culture in the University of Groningen, and English philology in the University of Helsinki. Currently she is writing her doctoral dissertation in the Finnish National Defence University, where she majors in leadership. Her research interests include language and identity, ideology in discourse, strategic communication and multimodal discourse. Jantunen currently works in education.