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