

Cyberspace: Definition and Implications

Rain Ottis, Peeter Lorents

Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

rain.ottis@ccdcoe.org

peeter.lorents@ccdcoe.org

Abstract

In recent years the term “cyber” has been used to describe almost anything that has to do with networks and computers, especially in the security field. Another emerging field of study is looking at conflicts in cyberspace, including state-on-state cyber warfare, cyber terrorism, cyber militias etc. Unfortunately, however, there is no consensus on what “cyberspace” is, let alone what are the implications of conflicts in cyberspace.

In order to clarify this situation, we offer the following definition: *cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems*. We describe the background of the definition and show why this approach may be preferable over others. Specifically, we revisit the terms coined by Norbert Wiener (the father of cybernetics) and William Gibson. We show that time-dependence is an overlooked aspect of cyber space and make a case for including it in our proposed definition.

In addition, we look at the implications that can be drawn from the time-dependence of cyberspace, especially in regard to cyber conflicts, which we define as *a confrontation between two or more parties, where at least one party uses cyber attacks against the other(s)*. Specifically we review the implications on the potential for rapid deployments of offensive and defensive actions in cyberspace, the feasibility of mapping cyberspace, and the need for constant patrolling and reconnaissance.

Keywords:

cyberspace, cyber conflicts, cyber attacks, time, definition

1. Introduction

Every once in a while a new term comes along or an old term gets a novel meaning and suddenly it is everywhere. In recent years (decades, arguably), the word “cyber” has been added to a long list of words to create “new” terms. Examples of terms that surface in academic papers include cyber society (Lorents 2009), cyber attacks (Ottis 2008), offensive cyber capability (Ottis 2009), cyber defense, cyber warfare, cyber crime, cyber terrorism, etc. They all have something to do with the concept of *cyberspace*, which is often the presumed context or environment for the cyber concept in question. It follows that it is very important to have a good definition for cyberspace or the derived terms may become meaningless or flawed.

Below we review the origins of the term cyberspace and look at some of the definitions offered for it today. Following the quick overview, we propose our own definition and explain why it may be preferable over others. We finish by drawing some implications from our definition in regards to conflicts in cyberspace.

2. Overview of definitions

The term *cyber* has evolved from the work of Norbert Wiener, who defined the term *cybernetics* in the title of his book as “*control and communication in the animal and the machine*” (Wiener 1948). The idea that humans can interface with machines and that the resulting system can provide an alternative environment for interaction provides a foundation for the concept of cyberspace.

In the early 1980’s the science fiction author William Gibson took the next step by coining the word *cyberspace* in one of his books. Even though this happened in a fictional setting, the word has become widely used in professional and academic circles. In his book, he described cyberspace as a “consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity.” (Gibson 1984) This definition focuses on the human perception

of the new environment, but is still very relevant, as it illustrates the potential for developing a truly immersive cyberspace experience. The second half of the definition identifies complexity as one of the principle characteristics of cyberspace.

Over the years, many different definitions have evolved for cyberspace. The US Department of Defense, for example, considers cyberspace as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” (JP 1-02) This definition is remarkable as it only refers to the (hardware) technology component, although software and data may be inferred from the wording. Noticeable is the lack of the human component, which is so important in Wiener’s and Gibson’s definitions.

The European Commission, on the other hand, vaguely defines cyberspace as “the virtual space in which the electronic data of worldwide PCs circulate”. (European Commission) Again, no reference is made to the human component while the technological component is restricted to data passing between personal computers. Arguably, online encyclopedias are a more likely source of definitions for the average “citizen” of cyberspace. Webopedia, for example, offers a definition similar to the previous one, claiming that cyberspace is a “metaphor for describing the non-physical terrain created by computer systems”. (Webopedia) Even though they are similar, their usefulness is limited because of vague terminology and concepts.

The Wikipedia, however, offers that cyberspace “is the global domain of electromagnetics as accessed and exploited through electronic technology and the modulation of electromagnetic energy to achieve a wide range of communication and control system capabilities.” (Wikipedia) Here we have a definition that includes the technology component, the human component (who accesses and exploits) and the communication and control component, which brings us back to Norbert Wiener’s definition of cybernetics.

Indeed, the variety seen in the definitions can be explained by the different viewpoints of the sources. As Strate (1999) illustrated, there is a rich taxonomy for describing cyberspace. He divided it into three tiers: zero order (ontology and cyberspacetime), first order (physical, conceptual and perceptual cyberspace) and second order cyberspace (synthesis of cybermedia space).

Even though there is a wide range of definitions from dictionary answers to state-approved terms to from-the-hip personal favorites, they mostly agree that the core of cyberspace consists of the globally connected networks of hardware, software and data. Another important aspect, which is usually not explicitly stated but can be inferred, is that humans can interface (although clumsily) with cyberspace and in doing so, become part of it. However, in order to better describe the notion of cyberspace and understand the complexity that comes with it, we must also take into account the time factor.

Time is notably absent from most definitions of cyberspace. A counterexample of this trend is the concept of cyberspacetime, which expands on the cyberspace term. “Cyberspacetime is the totality of events involving relationships between humans and computers, between humans through computers, and between computers themselves.” (Strate 1999) For our purposes, however, this does not address the dynamic nature of cyberspace, but seems to encompass the entire history of events in cyberspace in one giant static setting. Therefore, we propose our own definition for cyberspace.

3. Proposed definition

As the overview of definitions showed, there is no common definition for cyberspace and the ones that are used are often vague or missing key components. We have also identified that the definitions do not properly address the dynamic nature of cyberspace. In order to correct this we propose the following definition: *cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems.*

By interconnected information systems we mean the information (Lorents 2009), hardware, software and the media that connects them. A convenient way to model such systems is to use graphs, where nodes

represent computers, networking devices, sensors, user interfaces etc. and edges represent connections between nodes (cables, radio links, etc.).

Note that we have also included the human users in the definition. Cyberspace is an artificial space, created by humans for human purposes. Without human users cyberspace would stagnate, fall into disrepair and eventually – cease to be. Unless something else can take over the maintenance and development of cyber infrastructure and content, the human remains an important part of cyberspace.

Considering the amount of nodes in the global network, it becomes clear why cyberspace is considered “unthinkably complex”. The International Telecommunication Union estimates that nearly a quarter of the world’s population is using Internet, while over 60% are using mobile phones (ITU 2009). Supporting the user side is the core infrastructure of the networks, as well as the myriad service providers that allow people to communicate, shop, play, work – to live online.

However, the complexity increases even further if you consider that this network is not static. To highlight this issue, we have introduced the concept of *time-dependence* to our definition. Both elements and relations between elements can change (or remain unchanged) in time-dependent sets and systems as the time progresses (Lorents 2001). In cyberspace, this means that users, nodes and connections can appear and disappear, and information is transformed over time. Compared to other time-dependent systems, dramatic changes can take place in extremely short time in cyberspace. For example, a piece of malicious code can replicate, infect and effectively disable large parts of a global network in a matter of seconds or minutes.

The overview focused on the cyber part of cyberspace, but the second part of the term cyberspace – “space” – also requires some clarifying remarks. In exact and engineering sciences a space is not just any set of objects. In order to call something a space we must define the corresponding topology or metric (Kuratowski 1966). In the latter case it must be clear how the distance between elements is calculated, so that the metrics axioms are met (Deza 2006). It should be noted that several different metrics can be used on the same set of elements if the respective different distance calculation procedures are used.

It follows that there are many options for calculating distance in cyberspace. Without delving into the mathematical details, we note that in case of information systems, the “geographical” distance between nodes is probably not the most useful metric, especially considering the speed of information propagation in the system. Instead, considering that cyberspace can be modeled as a graph, we can use metrics from graph theory. For example, *distance between two nodes = shortest path between the two nodes* (Deza 2006).

4. Implications

Whether we consider cyberspace as an actual space or just a collection of resources, the actors in cyberspace (including states, businesses, organizations, groups and individuals) will compete for the control of it. As any space, cyberspace is also contested “ground”, which leads us to the inevitability of conflicts in cyberspace. Let us define a cyber conflict as *a confrontation between two or more parties, where at least one party uses cyber attacks against the other(s)*.

The nature of the conflict will differ based on the nature and goals of the participants. Criminals look for illegal revenue, so they hijack parts of cyberspace. Intelligence services look for useful information, so they attack enemy, friendly, or neutral parts of cyberspace to get access to that information. Militaries look to disrupt the operations of the enemy, so they attack the sensor, logistics, communications and control systems in enemy cyberspace. The conflicts can be as simple as civil disputes over domain name ownership or as complex as deliberate cyber attack campaigns as part of a conventional war between technologically advanced states.

Given the assumption that cyber conflicts are inevitable, we can draw several implications from the time-dependent aspect of cyberspace. The time-dependence is easiest to explain as *the change in the structure and content of cyberspace over time*. We have already pointed out that in cyberspace, the

relevant time span can be relatively short – minutes, often even seconds or fractions of a second. Based on this we can draw implications on the potential for rapid deployments of offensive and defensive actions, the feasibility of mapping cyberspace, and the need for constant patrolling and reconnaissance.

The quick changes in cyberspace imply that a relatively short amount of time is needed to carry out an attack or implement new defenses, compared to physical space. A self-replicating network worm can infect large parts of cyberspace in a matter of minutes. For example, in 2003 the SQL Slammer worm infected approximately 90% of the vulnerable hosts connected to Internet in just 10 minutes, to a total of about 75 thousand machines across all continents (Moore 2003). The only comparison to this in physical space is the simultaneous launch of hundreds or thousands of ballistic missiles armed with conventional warheads. Anything short of that will not have global consequences within a similar time span.

On the defensive side, in cyberspace it is possible to upgrade defenses in seconds or minutes by implementing new firewall rules, for example. Building a new concrete bunker or a Maginot line in physical space is much more time consuming. This does not mean that erecting defenses in cyberspace is or can always be done in minutes, however. It merely points out that it is possible to deploy prepared defensive measures (tighter firewall rules, alternative routing and hosting etc.) in a short amount of time.

In preparing for a cyber conflict it is necessary to be aware of the “terrain” of the potential conflict zone, the defensive and offensive capabilities of the actors and the possibility for collateral damage and unplanned escalation. Due to the nature of cyberspace, this is difficult to do, as the environment is complex and in constant change. Potential entry vectors, critical targets, key users and information can change within seconds. As a result, the map can only be near real-time at best and there is no way of ensuring that it will look the same on the day of the planned attack (or defense).

Based on this we can draw another implication. If the map is constantly changing, then “patrolling” and reconnaissance efforts must also be constant, as long as one is concerned about the possibility of a conflict in cyberspace. This means regular monitoring and entrapment operations on the defensive side and regular probes on the offensive side. Without it, an attack may go undetected or, in the offensive case, the attack may be thwarted by a simple change in target posture. This need for constant activity, however, raises the risk of detection for the attackers and it can betray the plans and routines of the defenders.

Conversely, fire-and-forget or deploy-and-forget type attacks and defenses quickly lose their effectiveness in cyberspace, as the opposing side reacts and adapts. As is true in maneuver warfare, an obstacle is not *really* an obstacle, unless it is covered by observation and fire. Similarly, if one does not upgrade one’s weapons, they will soon be unable to penetrate the armor of the enemy. Therefore, cyberspace requires constant vigilance from the planners and combatants.

Many of the examples above use analogies to explain the difference or similarity between conflicts in cyberspace and physical space. These are meant to serve as illustrations only and should be treated with some reservations. The potential problems with using and abusing metaphors and analogies in cyber topics have been demonstrated by Sulek and Moran (2009).

5. Conclusion

We have given a short overview and analysis of the evolution and common meaning of the term cyberspace and made a contribution by offering a new definition. We propose that *cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems*, where the addition of time-dependence is our contribution. We have also tried to analyze the implications of the time-dependence issue from a cyber conflict perspective. While this new definition does not necessarily replace any pre-existing definitions, we feel that it does offer an important viewpoint to cyberspace that is often not considered.

References

Deza E. and Deza M.M. (2006) *Dictionary of Distances*. Amsterdam, Elsevier.

Gibson, W. (1984) *Neuromancer*. New York, Ace Books.

European Commission. "Glossary and Acronyms (Archived)". In Information Society Thematic Portal, [online], http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c. [Accessed 03 Nov 2009]

International Telecommunication Union. (2009) "Measuring the Information Society". [online], http://www.itu.int/ITU-D/ict/publications/idi/2009/material/IDI2009_w5.pdf. [Accessed 03 Nov 2009]

Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms. (2009) [online], http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf. [Accessed 03 Nov 2009]

Kuratowski K. (1966) *Topology*. New York, Academic Press.

Lorents, P. (2001) *Informaatika teoreetilised alused* (Theoretical Foundations of Informatics). Tallinn, EBS Print.

Lorents, P. and Ottis, R. and Rikk, R. (2009) "Cyber Society and Cooperative Cyber Defence". In *Internationalization, Design and Global Development*. Lecture Notes in Computer Science, vol. 5623, pp. 180-186.

Moore, D. and Paxson, V. and Savage, S. and Shannon, C. and Staniford, S. and Weaver, N. (2003) "Inside the Slammer Worm". *IEEE Security and Privacy*, Vol 1, No 4, pp. 33-39.

Ottis, R. (2008) "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." In *Proceedings of the 7th European Conference on Information Warfare and Security*, Plymouth. Reading, Academic Publishing Limited, pp 163-168.

Ottis, R. (2009) "Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability." In *Proceedings of the 8th European Conference on Information Warfare and Security*, Lisbon. Reading, Academic Publishing Limited, pp 177-182.

Strate, L. (1999) "The Varieties of Cyberspace: Problems in Definition and Delimitation." *Western Journal of Communication*, Vol 63, No 3, pp. 382-412.

Sulek, D. and Moran, N. (2009) "What Analogies Can Tell Us About the Future of Cybersecurity". In Czosseck, C. and Geers, K (eds.) *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam, IOS Press, pp. 118-131.

Webopedia. "cyberspace". [online], <http://www.webopedia.com/TERM/c/cyberspace.html>. [Accessed 03 Nov 2009]

Wiener, N. (1948) *Cybernetics: Or Control and Communication in the Animal and the Machine*. New York, John Wiley.

Wikipedia. "Cyberspace". [online], <http://en.wikipedia.org/wiki/Cyberspace>. [Accessed 03 Nov 2009]