International Journal of Cyber Warfare and Terrorism
Volume 6 • Issue 1 • January-March 2016

Arts and Branches of Science Significantly Contributing to Cyber and Cyber Security:
The West European and the Russian Views

Margarita Levin Jaitner, Swedish Defence University, Stockholm, Sweden
Áine MacDermott, School of Computer Science, Liverpool John Moores University, Liverpool, UK

ABSTRACT

Academia plays an important role in shaping a country's cyber readiness. In the past years, nations have started investing in new cyber-related programs at colleges and universities. This also includes promoting academic exchange with partner countries, as well as putting effort into improved cooperation between industries and scholars in the area of cyber. In many cases the efforts focus largely on computer science and closely related branches of science. However, the very nature of the cyberspace as both a continuation and a reflection of the physical world require a broader perspective on academic assets required to create and sustain sound cyber defines capabilities. Acknowledging this premise, this paper sets out to map branches of science that significantly contribute to the domain known as 'cyber' and searches for new aspects for further development.

KEYWORDS

Computer Science, Cyber Security, Cyber, Education, Russia, Science, Western Europe

INTRODUCTION

Academia plays an important role in shaping a country's cyber readiness. In the past years, nations have started investing in new cyber-related programs at colleges and universities. This also includes promoting academic exchange with partner countries, as well as putting effort into improved cooperation between industries and scholars in the area of cyber. In many cases the efforts focus largely on computer science and closely related branches of science. However, the very nature of the cyberspace as both a continuation and a reflection of the physical world require a broader perspective on academic assets required to create and sustain sound cyber defines capabilities. Acknowledging this premise, this paper sets out to map branches of science that significantly contribute to the domain known as 'cyber' and searches for new aspects for further development.

This paper acknowledges scholarly contributions produced and published in English and Russian languages, which also allows the identification of a focal point that is set in the respective academic environment. The commonly used western definitions - especially when it comes to cyber security on a national level - rest upon the military definition of Computer Network Operations, or CNO. CNO is comprised of Computer Network Attacks (CNA), namely 'Operations designed to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves' (European Parliament, 2011), Computer Network Exploitation (CNE), which deals largely with retrieval of information or espionage, as well as Computer Network Defence (CND),

DOI: 10.4018/IJCWT.2016010103

which aims at defending own networks. CNO in turn can be used to conduct Information Operations (IO) (US Department of Defence, 2012/2014).

Russia on the other hand is known to define cyberspace in a somewhat different manner than western societies - cyberspace according to the Russian Cyber Security Strategy is far more than a network of computers but also an information space, a space for messages. Thus, control over cyberspace in the Russian view extends to content but merely only over technical systems (Ministry of Defence of the Russian Federation, 2011; Giles, 2012). This in turn integrates Information Operations (IO) within the realm of cyber security, rather than excluding and may - but does not necessarily have to - lead to a tighter integration with what is, from a western point of view, the responsibility of authorities tasked with IO, PSYOPS - Psychological Operations, and overall Strategic Communication (STRATCOM).

We establish the definition of 'cyber', as well as terminology to be used throughout the paper, acknowledging that academic and practical definitions in this area are still somewhat fluid. Academic education currently delivered in Western Europe and Russia is examined, and our findings from various studies regarding aspects of cyber education and its immersion into a nation's cyber readiness are discussed. Necessary and desirable points of cooperation between various branches of science are mapped out and highlighted, as we argue that a nation's cyber progression and readiness draws great benefits from broad interdisciplinary efforts. The results of the presented research can be of broad use for policy makers whenever it is necessary to assess to what extent cyber-related issues are covered academically within a nation. Furthermore, personnel tasked with creation and improvement of cyber-related academic programs will find use in these findings when developing comprehensive curricula.

THEORETICAL APPROACH

For the purpose of this paper, we describe the cyber domain - which ultimately touches upon a nation's cyber readiness - as one of five domains, or layers of cyber as highlighted in Figure 1 by the US Department of Defence. In contrast to the other four domains, the cyberspace is in its entirety constructed by humans. It is interconnected with the other domains through physical residence within all of them, which is why events in these domains have the power to greatly impact the cyberspace. The cyberspace can be described as consisting of three basic layers, although other descriptions, for example using more layers or different analogies are available. The first layer - physical - regards the physical structure of the cyberspace, its physical network components, as well as their geographical placement. The second layer is comprised of the logical network components - the logical connection between the physical units in the first layer. The third layer is inherently human and is comprised of persona components - humans in the network and their cyber persona such as network accounts, e-mail addresses, etc. (US Department of Defence, 2010).

Each of these layers is potentially vulnerable and requires its own knowledge set and capabilities in order to be protected. A potential adversary would attempt to identify the weak link in any of the layers, matching their own strength and capability, seeking to balance their own shortcomings in skills or assets against their enemy's weaknesses. In some cases the attacker may launch an attack that may appear as less serious on one layer, but on the other hand still greatly influence another layer. This can be exemplified by larger-scale DDoS attacks, technically seen, are little more than a nuisance. Such attacks, however, may extend into the social layer and actually influence humans in their behaviour and decision-making. Therefore, it is necessary for defenders to be able to grasp both the potential weaknesses of individual layers, as well as how the layers are interconnected. "*Simply*