

# Chapter 48

## 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, Sweden*

**Áine MacDermott**  
*Liverpool John Moores University, 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.*

### 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

DOI: 10.4018/978-1-5225-5634-3.ch048

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), 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

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/arts-and-branches-of-science-significantly-contributing-to-cyber-and-cyber-security/203544](http://www.igi-global.com/chapter/arts-and-branches-of-science-significantly-contributing-to-cyber-and-cyber-security/203544)

## Related Content

---

### Predicting Human Actions Using a Hybrid of ReliefF Feature Selection and Kernel-Based Extreme Learning Machine

Musa Peker, Serkan Balland Ensar Arif Saba (2018). *Handbook of Research on Predictive Modeling and Optimization Methods in Science and Engineering* (pp. 379-397).

[www.irma-international.org/chapter/predicting-human-actions-using-a-hybrid-of-relieff-feature-selection-and-kernel-based-extreme-learning-machine/206758](http://www.irma-international.org/chapter/predicting-human-actions-using-a-hybrid-of-relieff-feature-selection-and-kernel-based-extreme-learning-machine/206758)

### Proposals to Win the Battle Against Cyber Crime

Alaa Hussein Al-Hamami (2018). *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications* (pp. 1438-1453).

[www.irma-international.org/chapter/proposals-to-win-the-battle-against-cyber-crime/203570](http://www.irma-international.org/chapter/proposals-to-win-the-battle-against-cyber-crime/203570)

### Assembling of Parallel Programs for Large Scale Numerical Modeling

V.E. Malyskin (2012). *Computer Engineering: Concepts, Methodologies, Tools and Applications* (pp. 497-511).

[www.irma-international.org/chapter/assembling-parallel-programs-large-scale/62461](http://www.irma-international.org/chapter/assembling-parallel-programs-large-scale/62461)

### Delay Faults Testing

Marcel Baláž, Roland Dobaiand Elena Gramatová (2011). *Design and Test Technology for Dependable Systems-on-Chip* (pp. 377-394).

[www.irma-international.org/chapter/delay-faults-testing/51410](http://www.irma-international.org/chapter/delay-faults-testing/51410)

### Low-Power Methodologies and Strategies in VLSI Circuits

Preethi, Sapna R.and Mohammed Mujeer Ulla (2023). *Energy Systems Design for Low-Power Computing* (pp. 1-16).

[www.irma-international.org/chapter/low-power-methodologies-and-strategies-in-vlsi-circuits/319986](http://www.irma-international.org/chapter/low-power-methodologies-and-strategies-in-vlsi-circuits/319986)