Emily Vandalovsky

Literature Review

Fall 2017

New Jersey City University

Dr. Shamburg

EDTC 805

Global Issues in ET Leadership

Introduction

As cyber attacks increase in frequency, complexity, and severity around the globe, the need for a highly trained cybersecurity workforce is essential. Modern cybersecurity education is global in its nature and should be approached with a wider spectrum of disciplines, both technical and non-technical in nature. This paper discusses the cybersecurity education within the framework of national cybersecurity policies, describes the term cyber in the framework of cyberspace and cyber sciences and provides several examples for implementing the interdisciplinary approach in cybersecurity education. Additionally, it reiterates the growing need for cybersecurity professionals worldwide.

Review of Literature

National Priority. As with many other countries, cybersecurity is a national priority in the United States (The White House, 2017). According to the executive order on strengthening the cybersecurity of federal networks and critical infrastructure, signed by the President Trump on May 11, 2017, in order to grow and sustain the level of the national cybersecurity workforce in both private and public sectors, the appropriate entities must focus on the "efforts to educate and train the American cybersecurity workforce of the future, including cybersecurity-related education curricula, training, and apprenticeship programs, from primary through higher education" (The White House, 2017).

Global Nature of Cybersecurity

Similarly to US Government, the governments of other countries recognize the importance of cybersecurity education, as a part of their national and international cybersecurity strategies. A call to stronger cybersecurity education initiatives is prevalent in United Kingdom policy on National Cyber Security Strategy 2016-2021, the document outlining the country's approach to a more secure and resilient path in cyberspace. (UK Cabinet Office et al., 2016). Correspondingly, the government of Netherlands commits to obtaining sufficient cybersecurity knowledge and skills as one of the five listed objectives within the framework of the National Cyber Security Strategy (Netherlands National Cyber Security Center. 2013).

NATO contribution. Due to the global nature of cybersecurity, providing current and adequate cybersecurity education is globally recognized challenge and priority. A number of counties around the world share similar goals and concerns while developing and implementing a curriculum for cybersecurity education. To assist with the mutual challenges of cyber resilience and cyber education and to promote further collaboration on the international level, The North Atlantic Treaty Organization (NATO) established the Cooperative Cyber Defense Center of Excellence (CCDCOE). According to CCDCOE website, its "mission is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defense by virtue of education, research and development, lessons learned and consultation." (NATO Cooperative Cyber Defense Center of Excellence, 2017).

With the Internet being the catalyst of globalization and cyber interconnection, the cybersecurity efforts is nothing less of the international scope. With the assistance of Euro-Atlantic Partnership Council (EAPC), NATO's Mediterranean Dialogue, Istanbul Cooperation Imitative (ICI) and other global partners, CCDCOE provides a comprehensive collection of national and international cybersecurity policies, strategies, and legal documents from twenty-six NATO nations and fifty-seven Non-NATO nations. (NATO Cooperative Cyber Defense Center of Excellence, 2017). Together, over eighty nations have already developed and continue continuously upgrading their national and international cybersecurity legal documents.

Digital divide in cybersecurity. Governmental agencies throughout the globe recognize the importance of participation in the international initiatives on cybersecurity. (Hanson, 2009). However, in some cases, the field of cybersecurity contributes to the "digital divide" between developed and developing countries. (Westby, 2004). There are still a significant number of developing countries that find it difficult to keep up with the ever-growing threat of cyber attacks. They are challenged by creating national cybersecurity policies or, in some cases, by their implementation. (Newmeyer, 2015). Due to the lack of adequate legislative framework, human and technical resources, and proper levels of support, a number of developing countries are experiencing difficulties with establishing and providing the same levels of cybersecurity and cybersecurity education as a number of developed countries. (Newmeyer, 2015).

Defining the Plainfield

One of the commonly stated challenges of cybersecurity education lays within the definition of the field. The term cybersecurity implies the very act of securing or protecting from unauthorized use.   But what is it that needs to be protected? The list of individual answers could grow long, all of which could be covered by the umbrella of cyberspace. Over the years, multiple definitions of cyberspace emerged and/or have been altered several times by a number of organizations including Pentagon. (Singer & Friedman, 2014).

Cyberspace and human element. For the purposes of this paper, it is helpful to think of cyberspace as not only the Internet's infrastructure of networked computers, routers, fiber-optic cables, cellular technologies and traveling data, but also as people involved in implementing these processes and the decisions they make. In their book *Cybersecurity: what everyone needs to know*, Singer & Friedman state: "cyberspace is defined as much by the cognitive realm as by the physical and digital. Perceptions matter and they inform cyberspace's internal structures in everything from how the names within cyberspace are assigned to who owns which parts of the infrastructure that powers and uses it." (Singer & Friedman, 2014, p.14).

The human dimension of the cyberspace, and more specifically, its role within cybersecurity framework, is further explored by the team of faculty members from the University of Central Florida, Institute of Simulation and Training, in their efforts to create a pilot program with the human-centric approach to cyber education. (Caulkins et al., 2016) The importance of such approach towards cyberspace becomes more apparent nowadays, as human element continues to be considered one of the most critical components of cyber operations. (Champion et al., 2014).

NATO resources. Along with multiple viewpoints at the definition of cyberspace, a degree of fluctuation exists in the interpretation of other cyber-related terms. In the attempt to create a shared knowledge base and provide a common denominator for the information exchange as well as respectfully incorporate existing points of view, an inclusive collection of cyber definitions has been created by NATO Cooperative Cyber Defense Center of Excellence and published resources page on the website. (NATO Cooperative Cyber Defense Center of Excellence, 2017).

Holistic Approach

In order to provide the adequate framework for the current review, I will focus on the holistic approach to the connotation of the term cyber in the educational setting. According to Cyber Education Project (CEP), the organization, comprised of academia representatives and computing professionals and focused on the development of undergraduate curriculum guidelines, a holistic approach to cyber education is described by "cyber sciences" in the following way:

> The term "Cyber Sciences" reflects a collection of computing-based disciplines involving technology, people, and processes aligned in a way to enable "assured operations" in the presence of risks and adversaries. It involves the creation, operation, analysis, and testing of secure computer systems (including network and communication systems) as well as the study of how to employ operations, reasonable risk taking, and risk mitigations. The concept of "Cyber Sciences" refers to a broad collection of such programs, and disciplines under this umbrella often also include aspects of law, policy, human factors, ethics, risk management, and other topics directly related to the success of the activities and operations dependent on such systems, many times in the context of an adversary. (Cyber Education Project, 2017).

Historic perspective. The inclusive or holistic approach to cybersecurity education is not an entirely new concept. Several years ago, when the field was mostly referred to as Information Assurance, it was already perceived, although not as widely as nowadays, as a joint educational effort. In 2003, in his publication on *Information system security curricula development*, Ed Crowley wrote the following about the Information Assurance: “IA is multidisciplinary. Within an organization, IA is dependent upon computing infrastructure, policies, and people. Consequently, IA as a discipline includes aspects of diverse disciplines including psychology, sociology, law, computer engineering, and management.” (Crowley, 2003).

Multidisciplinary Approach. With a wide spectrum of cyber-related topics and a multifaceted nature of the field, a number of various global entities from governmental to academic to professional sectors were able to recognize the importance of the multidisciplinary approach towards cybersecurity education. The inclusive understanding of cyber field broadens the approach to cyber education by incorporating technical and non-technical fields, both of which are equally important. (Kam & Katerattanakul, 2014).

American examples. A number of institutions in the United States already adapted such approach and were able to implement a multidisciplinary framework for cybersecurity education on both undergraduate and graduate levels. The Department of Computer Science at the University of Texas-Pan American reports the following about its Master's in Interdisciplinary Studies program: "taking a multidisciplinary approach to security and more particularly cyber security results in graduates who can think more openly and within alternative systems of thought. They are able to recognize and assess assumptions, implications and particular consequences." (Lawrence-Fowler, 2013). Some educational institutions implement a multidisciplinary approach towards cybersecurity education on the undergraduate level. For instance, Salve Regina University of Newport, RI, is reportedly the only Rhode Island institution to create an opportunity for all its undergraduate students to receive an interdisciplinary cybersecurity education by implementing a 15-credit concentration in cyber resiliency. (Salve Regina University. 2017).

International studies. On the international arena, a comparable holistic approach to cybersecurity education has been recognized and recommended by a number of researchers. In their study on *Cyber security education in Montenegro: current trends, challenges and open perspectives* a group of scholars from University of Donja, Montenegro, recommends that "[p]rograms must teach a combination of theory and practice, and to have a holistic approach; Cybersecurity should be taught in an integrated fashion, with all students learning basic principles and respect principle of the interdisciplinary" (Šendelj & Ognjanović, n.d.).

A similarly inclusive approach has been reviewed and recommended by a group of researchers from the Delft University of Technology, Netherlands. In the article *On (the emergence of) cyber security science and its challenges for cyber security education,* the group discusses the complex nature of the modern cybersecurity field, which requires a broader view inclusive of technical and non-technical fields. (Van den Berg, 2014). The article states, that "[n]ext to technical issues, attention should be paid to all kinds of non-technical issues including governmental, behavioral, legal/ethical, and economic aspects" (Van den Berg, 2014).

Key to Innovation

Some governing bodies, like Ministry of Security and Justice of Netherlands, recognize the importance and include the multidisciplinary approach to cyber education into their national cybersecurity strategy. Not only does the Netherlands Government identify the importance of the multidisciplinary approach to the overall cyber education and the increased interest in the field, but it also recognizes its role in innovation and expansion beyond the technical areas. (Netherlands National Cyber Security Center, 2013) As the National Cyber Security Strategy report, published by National Cyber Security Center of the Ministry of Security and Justice of Netherlands, states: "[a] multidisciplinary approach in which the non-technical sub-areas are also included is needed to promote cyber security innovation. The innovative products and services that are developed in this manner will help the Netherlands with anticipating swift technological and other developments in the digital domain." (Netherlands National Cyber Security Center, 2013, p.26).

Gap between Supply and Demand

Most educational programs in cybersecurity share one common goal: to train the professionally skilled workforce. While educational levels, times of completion and geographical locations may vary, the programs in cybersecurity education focus on one common goal: to fulfill the industry demands with knowledgeable and skilled graduates.

In the United States, there were 100,000 information security analyst positions available nationwide in 2016, and the US Department of Labor projected this number to grow at the rate of 28% through 2026. (Bureau of Labor and Statistics, 2017). According to CyberSeek, there are over 19,000 cybersecurity job positions open in the metro area of NY-NJ-PA, with nearly 10,000 open positions in the state of New Jersey alone (CyberSeek, 2017). On the global scale, the demand for cybersecurity professionals is measured in millions. According to Vogel, the global number of jobs by 2020 will reach 1.5 million, which illustrates a tremendous level of need. (Vogel, 2016).

As does the US Government, governments of other counties recognize the gap between supply and demand in the field of cybersecurity and focus on shortening it. For instance, the United Kingdom states the following in its National Cyber Security Strategy policy paper, “The UK needs to tackle the systemic issues at the heart of the cyber skills shortage: the lack of young people entering the profession; the shortage of current cyber security specialists; insufficient exposure to cyber and information security concepts in computing courses; a shortage of suitably qualified teachers; and the absence of established career and training pathways into the profession”. (UK Cabinet Office et al., 2016, p.55).

Due to its encompassing scope and global nature, cybersecurity education is approached as inclusive, broader initiative incorporating a spectrum of fields and educational disciplines. This notion is shared by a number of governments, as supported by their national cybersecurity strategies as well as groups of academic researchers and pilot educational programs.   Driven by the worldwide growing demand for industry professionals in public and private sectors, the multidisciplinary approach to cybersecurity is to contribute to closing a gap between the supply and demand in cybersecurity workforce.

References:

Bureau of Labor and Statistics, U.S. Department of Labor. (2017, October 24). *Occupational Outlook Handbook*, Information security analysts. Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Caulkins, B. D., Badillo-Urquiola, K., Bockelman, P., & Leis, R. (2016, October). Cyber workforce development using a behavioral cybersecurity paradigm. In *Cyber Conflict (CyCon US), International Conference on* (pp. 1-6). IEEE. Retrieved from https://www.researchgate.net/profile/Bruce_Caulkins/publication/320433920_Modeling_and_Simulation_Education_for_Behavioral_Cybersecurity/links/59f7289a0f7e9b553ebd5b68/Modeling-and-Simulation-Education-for-Behavioral-Cybersecurity.pdf

Champion, M., Jariwala, S., Ward, P., & Cooke, N. J. (2014, September). Using Cognitive Task Analysis to Investigate the Contribution of Informal Education to Developing Cyber Security Expertise. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 58, No. 1, pp. 310-314). Sage CA: Los Angeles, CA: SAGE Publications.

Crowley, E. (2003, October). Information system security curricula development. In *Proceedings of the 4th conference on Information technology curriculum* (pp. 249-255). ACM. Retrieved from: http://www.geocities.ws/crowleye3919/pdf/Security_CITC.pdf

Cyber Education Project. (2017). *About Us*. Retrieved from https://cybereducationproject.org/about

CyberSeek. (n.d.). *Cybersecurity supply/demand heat map*. Retrieved from http://cyberseek.org/heatmap.html

Hanson, E. (2009). *A network of nations: Why effective cybersecurity requires international collaboration* (Order No. 1470408). Available from ProQuest Dissertations & Theses Global. (304886803). Retrieved from https://search.proquest.com/docview/304886803?accountid=12793

Kam, H. J., & Katerattanakul, P. (2014, October). Diversifying cybersecurity education: A non-technical approach to technical studies. In *Frontiers in Education Conference (FIE), 2014 IEEE* (pp. 1-4). IEEE. Retrieved from https://pdfs.semanticscholar.org/d8b7/817f66ec8e4e359bd99777e755f465da7f21.pdf

Lawrence-Fowler, W. A. (2013, January). Multi-disciplinary Approach to Cyber Security Education. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 1). The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). Retrieved from http://weblidi.info.unlp.edu.ar/WorldComp2013-Mirror/p2013/SAM9783.pdf

NATO Cooperative Cyber Defense Center of Excellence. (2017). *Cyber Security Strategy Documents*. Retrieved from https://ccdcoe.org/cyber-security-strategy-documents.html

NATO Cooperative Cyber Defense Center of Excellence. (2017). *Resources*. Retrieved from https://ccdcoe.org/cyber-definitions.html

Netherlands National Cyber Security Center. Ministry of Security and Justice. (2013). *National cyber security strategy 2: from awareness to capability*. Retrieved from https://www.ncsc.nl/english/current-topics/national-cyber-security-strategy.html

Newmeyer, K. P. (2015). Elements of National Cybersecurity Strategy for Developing Nations. *National Cybersecurity Institute Journal*, 9. Retrieved from http://www.excelsior.edu/static/journals/nci-journal/1-3/offline/download.pdf#page=11

Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011, October). The role of cyber-security in information technology education. In *Proceedings of the 2011 conference on Information technology education* (pp. 113-122). ACM. Retrieved from https://pdfs.semanticscholar.org/64c0/902ba8086bd6f7d8901cd8a72c275023b67c.pdf

Salve Regina University. (2017, October 25). *Interdisciplinary concentration in cyber resiliency designed for students in all majors*. Retrieved from http://www.salve.edu/news/interdisciplinary-concentration-cyber-resiliency-designed-students-all-majors

Šendelj, R., & Ognjanović, I. Cyber security education in Montenegro: current trends, challenges and open perspectives. Retrieved from http://ecesm.net/sites/default/files/EDULEARN_Sendlej.Ognjanovic.pdf

Singer, P. W., & Friedman, A. (2014). Cybersecurity: what everyone needs to know. Oxford University Press.

The White House. (2017, May 11). *Presidential executive order on strengthening the cybersecurity of Federal networks and critical infrastructure*. Washington, DC: White House. Retrieved from Office of the Press Secretary https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal

UK Cabinet Office, National security and intelligence, HM Treasury, and The Rt Hon Philip Hammond MP. (November 1, 2016). *National Cyber Security Strategy 2016 to 2021*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Van den Berg, J., Van Zoggel, J., Snels, M., Van Leeuwen, M., Boeke, S., Van de Koppen, L. & De Bos, T. (2014). On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. In *Proceedings of the NATO IST-122 Cyber Security Science and Engineering Symposium* (pp. 13-14).Retrieved from https://www.csacademy.nl/images/MP-IST-122-12-paper-published.pdf

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, *4*(2), 32. Retrieved from https://www.researchonline.mq.edu.au/vital/access/services/Download/mq:45093/DS01

Westby, J. R. (2004). International guide to cyber security. American Bar Association.