Guest Editorial Preface

Special Issue on Cyber Security

Eugenie de Silva, University of Leicester, Leicester, UK

The technologically dependent nature of the twenty-first century has resulted in rapid societal improvements. However, the revolutionary dynamics of this time period, whilst useful in exploring endless possibilities for global development, have also led to greater issues in the security domain.

For those working in the security arena, maintaining and strengthening cyberspace is especially imperative as terrorists and other criminals continue to improve their technical abilities. Yet, the necessity of cyber security also spans beyond national security into the commercial industries. Thus, cyber threats not only affect those with whom the responsibilities of protecting a nation at its core are allocated, but they also affect business entities and private citizens. With this taken into consideration, a greater awareness of cyber security has steadily grown to be an essential component of the global infrastructure.

The bounds of cyberspace could essentially be deemed as limitless. In 2014, the United Nations International Telecommunications Union reported that approximately three billion individuals around the world used the Internet; whilst the growth in these figures has steadily slowed in 2015 and 2016, the mammoth size of cyberspace is unquestionable and the uncertain bounds of cyberspace further make enforcing the law, especially transnationally, a difficult task.

Coordinating transnational law enforcement activities in the cyber arena is an issue that plagues many law enforcement agencies. How, when, and where can cyber criminals be prosecuted, and how can these criminals be pursued when they act under the guise of anonymity? These questions spotlight only a portion of the issues with which cyber security officials are faced, yet even these questions alone provide one with the opportunity to understand the inherent difficulties of monitoring and securing cyberspace.

To gain an understanding of the extent to which the topic of cyber security requires complex analyses and discussions, researchers and academics have placed a priority on further exploring and improving the discipline across the globe. In the United States of America (USA), there are programs, such as CyberCorps, which are aimed at providing full scholarships that cover "tuition, books, and professional development and include a cash stipend of $20,000 to $30,000 a year," for those students who focus on cyber security and would ultimately work for the USA government upon completion of their programs (Lawrence, 2014). In China, in March of 2016, the first Non-Profit Organization was founded to "support the safety and development of the Internet" (Xinhua, 2016). Additionally, in England, in March of 2016, the UK's new national cyber centre initiated collaborations with the Bank of England for "new cyber security guidance for financial firms" (The Register, 2016). Although there are many more examples that could be drawn to attention, these three examples show how different regions are equally strengthening their cyber security forces, albeit in various manners. It is for this reason that one could argue that researchers must be actively engaged in analyses within the discipline.

Researchers, academics, and even practitioners must conduct thorough investigations into the topic, so that the future of cyber security is not simply a trial and error process. The future of cyber security must be meticulously planned and organized in a manner that will minimize security breaches, enhance risk assessments, and ensure the privacy of data.

Intelligence and security are relatively novel fields with regard to academia; however, cyber security, as a distinct subject, is worthy of academic recognition, due to its complexity and academic rigor. In this *International Journal of Public Administration in the Digital Age*, this special issue of cyber security plays an important role in highlighting the diversification of the field, and providing an understanding of various facets of cyber security. Cyber security may justly be brought into the spotlight with the discussion of ISIL hacking and online propaganda, or the unlocking of the San Bernardino shooter's iPhone to gather data, but it is necessary to further emphasize the interwoven nature of cyber security in daily circumstances. Cyber security is not simply a field that requires pragmatic, hands-on experience with technical knowledge, nor is it a field that is only worthy of news attention when it relates to terrorism or radicalism. It is a field that requires a theoretical and historical understanding that allows for creative awareness of issues and solutions, and deserves public spotlight at all levels. By sharing theoretical and academic discussions, those involved are made aware of the multi-faceted nature of the field and are able to identify distinct ways in which to ensure that past mistakes and cyber security failures are not repeated. The papers in this special issue have been put through a double-blind, peer review, which has resulted in the presentation of high-quality work and contributions to the field. The authors of these articles, experts in their fields, have diligently worked to provide readers with understandings of varying facets of cyber security in a manner that enables individuals of all backgrounds to understand and become more aware of the diversity and intricacies of the discipline.

In its entirety, cyber security is a topic that has seemingly been provided with superficial media attention. The discipline is interwoven into daily activities; hence, it is unfortunate that media coverage and spotlight of this discipline has a tendency to focus on aspects that do not truly reveal the unique dynamics of the field. With this taken into consideration, it is fortunate that the five authors who have contributed to this special issue have adopted diverse, distinct perspectives, and have shared them in the hopes of strengthening the field in the academic arena, whilst providing individuals with the opportunity to understand cyber security in a pragmatic and clear manner.

Eugenie de Silva
Guest Editor
IJPADA

REFERENCES

Lawrence, D. (2014). *The US Government Wants 6,000 New 'Cyberwarriors' by 2016.* Retrieved 10 December, 2015 from http://www.bloomberg.com/news/articles/2014-04-15/the-u-dot-s-dot-government-wants-6-000-new-cyberwarriors-by-2016

The Register. Out-Law. (2016). *New UK Cyber Security Centre to Work with Bank of England.* Retrieved 03 December, 2015 from http://www.theregister.co.uk/2016/03/23/new_uk_cyber_security_centre_to_work_with_bank_of_england/

Xinhua. (2016). *China's First National NPO in Cyber Security Founded.* Retrieved 21 November, 2015 from http://news.xinhuanet.com/english/2016-03/25/c_135223674.htm

Eugenie de Silva holds a Bachelor's degree and Master's degree in Intelligence Studies with a concentration in Intelligence Analysis from the American Military University. She also holds a Master of Liberal Arts in Extension Studies with a concentration in Legal Studies from Harvard University. She also recently earned an MPhil in Education, Globalization, and International Development from the University of Cambridge. She has given eight oral presentations at academic conferences in fields, such as teaching physics and chemistry, online software programs, biometrics, intelligence studies, and Denial and Deception (D&D). Her research is mainly multidisciplinary in nature. She also holds the world record for being the youngest person to graduate with a Bachelor's degree in Intelligence Analysis at the age of fourteen. She is also recognized as Harvard's youngest graduate at the age of sixteen with a Master's degree.