Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2020 Proceedings | Southern (SAIS)

Fall 9-11-2020

Cybersecurity and Information Science: Towards a More Holistic and Interdisciplinary Approach

Unal Tatar
University at Albany State University of New York, utatar@albany.edu

Abebe Rorissa
University at Albany, State University of New York, arorissa@albany.edu

Dawit Demissie
Fordham University, ddemissie@fordham.edu

Follow this and additional works at: https://aisel.aisnet.org/sais2020

Recommended Citation

Tatar, Unal; Rorissa, Abebe; and Demissie, Dawit, "Cybersecurity and Information Science: Towards a More Holistic and Interdisciplinary Approach" (2020). *SAIS 2020 Proceedings*. 40.
https://aisel.aisnet.org/sais2020/40

This material is brought to you by the Southern (SAIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in SAIS 2020 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

CYBERSECURITY AND INFORMATION SCIENCE: TOWARDS A MORE HOLISTIC AND INTERDISCIPLINARY APPROACH

Unal Tatar
University at Albany State University of New York
utatar@albany.edu

Abebe Rorissa
University at Albany, State University of New York
arorissa@albany.edu

Dawit Demissie
Fordham University
ddemissie@fordham.edu

ABSTRACT

Cybersecurity is an emerging field of research and education with almost zero unemployment. Although cybersecurity is considered as a technical field, most of the problems in cybersecurity remain due to lack of an interdisciplinary perspective which handles issues by considering people and process aspects alongside technology. The information systems & science disciplines can partially address these issues with their established theories, tools, and methods and help develop a qualified workforce. This paper reports findings of a content analysis of the programs, specializations, and courses offered in 25 information schools to ascertain the extent to which the schools are ready to adopt cybersecurity in their curricula.

Keywords

Cybersecurity, information assurance, socio-technical, education

EXTENDED ABSTRACT

Cybersecurity (or information security, or information assurance) is an emerging field and profession, which suffers from a lack of adequate level of workforce. In the United States, there are almost 504,000 cybersecurity jobs available as of January 2020 (Cyberseek, 2020), while the total employed workforce is around 1 million. In addition, the demand for cybersecurity workforce has increased by over 50 percent since 2015. The rising demand for cybersecurity professionals is not just an issue for the United States. It is a global problem. What is more, the trajectory shows that the demand will be higher in the coming years (Crumpler & Lewis, 2019).

Cybersecurity is mostly considered a technical field. It is true that the cyberspace relies on a technology layer and its security has technical dimensions. However, cybersecurity is more than technology. Cybersecurity requires addressing problems from a socio-technical systems perspective, which includes people and process perspectives besides the technology perspective (Malatji, Von Solms, and Marnewick, 2019). Information systems and science, with their methods and theories emphasizing information, people, process, technology, organizations, and their interactions, can provide the desirable interdisciplinary perspective for cybersecurity education and research. This paper aims to examine if information science schools and programs include cybersecurity curricula to respond to the apparent need for a holistic and interdisciplinary cybersecurity teaching and research.

We conducted a content analysis of programs at 20 information science schools in the United States. The scope of our analysis includes courses, specializations, and programs in cybersecurity, information security, or information assurance offered at information schools. We identified several keywords (e.g., forensics, risk analysis, cyber law, privacy, cryptography, network security) to decide if a course or concentration or program is relevant to our study. We also utilized the *specialty areas* and *knowledge/skills/abilities* identified in the NICE Cybersecurity Workforce Framework (Newhouse, Keith, Scribner, and Witte, 2017) to guide our content analysis of descriptions of cybersecurity programs, concentrations, and courses.

Our analysis revealed the following findings: (1) Information schools in the United States have started to offer cybersecurity courses, specializations, and programs. Although there are quite a few courses related to cybersecurity, there are a very limited number of programs and concentrations in this field. (2) Most of the cybersecurity programs and specializations are at the graduate level (i.e., graduate certificate, master's, and Ph.D.) (3) Most of the cybersecurity courses offered at the Information Schools are at the undergraduate level. (4) The courses offered, which include risk analysis, network security, cryptography, cybercrime, cyber law, and data privacy, reflect the interdisciplinarity of the information science discipline.

REFERENCES

1. Cyberseek. (2020). Retrieved from https://www.cyberseek.org/.
2. Crumpler, W., & Lewis, J. A. (2019). The cybersecurity workforce gap. *Center for Strategic and International Studies, Washington, DC.[Online]. Available: https://www. csis. org/analysis/cybersecurityworkforce-gap*.
3. Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security*.
4. Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Special Publication*, *800*, 181.