Editorial

Special Issue on Cybersecurity, Cybercrime, Cyberwar

DOI 10.1515/jhsem-2014-1005

In the last two decades, we have witnessed tremendous technological advances in computing, communications, hardware and software technologies all of which continue to fuel the development, growth and importance of cyberspace. Today, governments and corporations depend heavily on cyberspace for many of their daily business activities and operations. Cyberspace is also playing an important role in the personal lives of citizens from around the world. The safety, economic stability and prosperity of society currently heavily depend on a safe, secure, reliable, and resilient cyberspace. The protection of cyberspace has become a national priority of many nations. The United States National Academy of Engineering has previously identified the securing of cyberspace as one of the 14 grand challenges of engineering in the 21st century (National Academy of Engineering 2008).

Cyberdefenders face significant challenges as they strive to protect cyberspace. Technical cybersecurity solutions alone are inadequate to address these challenges (Zeadally et al. 2013). We need strong collaborative partnerships among all of the various stakeholders including citizens, government, industry and academia to develop scalable cybersecurity solutions, cybersecurity policies and appropriate laws that can defeat a range of cyberthreats, cyberattackers and cybercriminals (Shore et al. 2011). Cyberspace is now considered as the fifth domain of war. It is still not clear what really defines the term cyberwar. Some have defined threshold requirements such as the number and type of cyberattacks that must be met before such attacks are considered cyberwar. Cyberwar issues are expected to continue to attract the attention of nations as they unleash both defensive and offensive cyber operations (Flowers and Zeadally 2014). The goal of this special issue is to present state-of-the-art research results in the areas of cybersecurity, cybercrime, and cyberwar.

"A Criminological Perspective on Power Grid Cyberattacks: Using Routine Activities Theory and Rational Choice Perspective to Explore Adversarial

Guest Editor: Sherali Zeadally, College of Communication and Information, University of Kentucky, USA, e-mail: szeadally@uky.edu