Cyber Warfare: Espionage, Botnet

Mr. Sharan L. Pais, Shrihstha, Shrikara R M, Shruthi C S, Sudheepa Poojari
Department of Information Science and Engineering
Alva's Institute of Engineering and Technology, Mijar, Moodbdri, Karnataka

Abstract: *The essential act of war is destruction, not necessarily of human lives, but of the products of human labour. The topic of cyber warfare is a vast one, with numerous sub topics receiving attention from the research community. We first examine the most basic question of what cyber warfare is, comparing existing definitions to find common ground or disagreements. Recent years have shown us the importance of cybersecurity. Especially, when the matter is national security, it is even more essential and crucial. Increasing cyberattacks, especially between countries in governmental level, created a new term cyber warfare. Creating some rules and regulations for this kind of war is necessary therefore international justice systems are working on it continuously. priority over the last decade, the Human Factors community has yet to approach it with critical mass.*

Keywords: Cyber War, Cyber Warfare, Law.

REFERENCES

[1]. V. D. Cha, "What do they really want? Obama's North Korea conundrum," *The Washington Quarterly*, vol. 32, no. 4, pp. 119–138, Oct. 2009.

[2]. NATO Review Magazine, "Cyber Timeline," in *North Atlantic Treaty Organization*. [Online]. Available: http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm. Accessed: Feb. 9, 2016.

[3]. R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," in *IEEE Xplorre*, vol. 9, IEEE, 2011, pp. 49-51. [Online]. Available:http://ieeexplore.ieee.org/stamp/st amp.jsp?tp=&arnumber=5772960. Accessed: Feb. 9, 2016.

[4]. D. Kushner, "The Real Story of Stuxnet," in *IEEE Spectrum*, 2013. [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-ofstuxnet. Accessed: Feb. 9, 2016.

[5]. S. J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," 2009.

[6]. S. Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security*, vol. 4, no. 2, pp. 49–60, 2015.

[7]. D. Hollis, "Cyberwar Case Study: Georgia 2008," in *Small War Journal*, 2011.

[8]. J. A. Lewis, "Computer Espionage, Titan Rain and China," Center for Strategic and International Studies, 2005.

[9]. C. Tankard, "Advanced Persistent Threats and how to Monitor and Deter Them," *Network Security*, vol. 2011, no. 8, pp. 16–19, Aug. 2011. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1353485811700861. Accessed: Feb. 10, 2016.

[10]. Google Official Blog, "A New Approach to China," Official Google Blog, 2010. [Online]. Available: https://googleblog.blogspot.com.tr/2010/01/ new-approachto-china.html. Accessed: Feb. 10, 2016

[11]. E. Hanford, "The Cold War of Cyber Espionage," in *Heinonline*, 2014. [Online]. Available: http://heinonline.org/HOL/Page?handle=hei n.journals/pilr20&div=9&g_sent=1&collecti on=journals. Accessed: Feb.10, 2016.

[12]. D. T. Kuehl, Cyberpower and National Security, Potomac Books and 1630 National Defense Univerity, 2009, Ch. From Cyberspace to Cyberpower: Defining the Problem, pp. 24 -42.

[13]. L. Alford, Cyber warfare: A new doctrine and taxonomy, US Air Force, accessed 25/05/14 (April 2001).

DOI: 10.48175/IJARSCT-5819