Hacktivism and Its Impact on Society

TREO Talk Paper

Miloslava Plachkinova, PhD
University of Tampa
mplachkinova@ut.edu

Au Vo, PhD
Loyola Marymount University
auvo1001@gmail.com

Abstract

Hacktivism is the intersection between activism and hacking. It covers operations that use hacking techniques against a target with the intent of disrupting normal business operations without causing as serious damages as cyberterrorism (Denning 2001). However, according to Coleman (2011) hacktivists engage more frequently in illegal, rather than legal, computer activities. There are various types of illegal activities, for instance, web sit-ins and virtual blockades such as distributed denial of services (DDoS attacks), automated email bombs, web hacks, computer break-ins, computer viruses, and worms. All together, they are different forms of electronic civil disobedience (ECD). In the era of social media and increased technology integration, hacktivism has been considered a new way to express civil disobedience (Delmas 2018).

While the damages caused by hacktivism may not seem as devastating as those caused by cyberterrorism, hacktivism has risen in prominence and popularity. It has crossed national borders and is considered a tool for influencing foreign policy (Denning 2001). It may seem tempting to think of hacktivists as vigilantes who serve the weak and underrepresented, or the 99% (Smallridge et al. 2016). However, we have to consider the socioeconomic impact of their actions. When it comes to hackers' motivation, there are three main dimensions: socio-cultural, economic, and political (Gandhi et al. 2011).

The Arab Spring is an example of how technology can be utilized to address complex global political problems. Anonymous, a decentralized international hacktivist group, provided an outlet for many oppressed citizens to express their opinion and to seek social justice. In addition to the social impact, we have to consider the financial implications of hacktivism. It is difficult to quantify the monetary value of inoperable, defaced, and down websites, leading to ruined reputation, and loss of political stability. Some studies show the growing concern of cyberattacks motivated by political and social causes (Bergal 2017). Fazzini (2017) also provided support for the growing trend, warning companies and governments to strengthen their security. Thanks to the prevalence of technology, is a general agreement that these attacks and their associated costs are only going to rise. Thus, we need to further explore these types of attacks.

References

Bergal, J. 2017. "Hacktivists Launch More Cyberattacks against Local, State Governments." Retrieved 09/21, 2018, from https://www.pbs.org/newshour/nation/hacktivists-launch-cyberattacks-local-state-governments

Coleman, G. 2011. "Anonymous: From the Lulz to Collective Action. The New Everyday." Retrieved 10/12, 2018, from http://mediacommons.org/tne/pieces/anonymous-traveling-pure-lulz-land-political-territories

Delmas, C. 2018. "Is Hacktivism the New Civil Disobedience?," *Raisons politiques*:1), pp. 63-81.

Denning, D. E. 2001. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," *Networks and netwars: The future of terror, crime, and militancy* (239), p. 288.

Fazzini, K. 2017. "Rising Hacktivist Attacks Take Companies by Surprise." Retrieved 10/12, 2018, from https://www.dowjones.com/insights/rising-hacktivist-attacks-take-companies-surprise/

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., and Laplante, P. 2011. "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political," *IEEE Technology and Society Magazine* (30:1), pp. 28-38.

Lohrmann, D. 2017. "The Dramatic Rise in Hacktivism." Retrieved 10/12, 2018, from https://techcrunch.com/2017/02/22/the-dramatic-rise-in-hacktivism/

Smallridge, J., Wagner, P., and Crowl, J. N. 2016. "Understanding Cyber-Vigilantism: A Conceptual Framework," *Journal of Theoretical & Philosophical Criminology* (8:1).