Online Activism to Cybercrime

Anita W. McMurtry
Atlanta Metropolitan State College, USA

Larry D. Stewart
Atlanta Metropolitan State College, USA

Curtis L. Todd
Atlanta Metropolitan State College, USA

INTRODUCTION

Hacktivism is a socially or politically motivated act of misuse of computer systems, the internet, or a technology hack; which can be traced three decades back to 1989, when DOE, HEPNET and SPAN (NASA) connected VMS machines worldwide and were penetrated by the anti-nuclear WANK worm (Moore, Shannon, & Brown, 2002). Subsequently, it appeared on criminal justice systems' radar from law enforcement, to the courts, and then to corrections. There is a new imperative to not only gain a better understanding of the intricacies of this problematic behavior when it rises to criminal activity, but also how best to safeguard society in general, as well as national and international public and private businesses, organizations and governmental agencies. This entry moves beyond mere definitions of how what was once considered another form of legitimate protest and activism by delving deeply into the psychology and practical ramifications of its emergence, which has quickly morphed into problematic cyber behavior and criminal activity perpetrated through the improper use of technological tools and digital platforms.

To construct a solid operational understanding of Hacktivism, this entry first extends its context as a cybercrime to include a global perspective, as well as hacker cultural and ethical mindsets. Second, inherent dangers, as it relates to critical areas such as political elections, industry and corporations, international affairs, personal data, and national security, are explored to further contextualize Hacktivism's evolution and real-world challenges in identifying, investigating and prosecuting criminals. Also, legal issues and implications for criminal justice systems are explored to firmly anchor the urgency in moving this virtual issue to the center of priorities. Finally, informed suggestions, recommendations and future research directions are provided.

HACKTIVISM: A CONTEXTUAL DEFINITION

Derived from combining the words "hack" and "activism", the term "Hacktivism" was first coined in 1996 by Omega, a member of the hacker collective Cult of the Dead Cow (Dyer, 2018). The group created an organization espousing that freedom of information was a basic human right. The group designed software to circumvent censorship controls on the Internet that some governments used to prevent citizens from seeing certain content. Hacktivism is mainly portrayed in society as the transposition of demonstrations, civil disobedience, and low-level information warfare into cyberspace (Dyer, 2018). Hacktivists

DOI: 10.4018/978-1-5225-9715-5.ch022

are the modern equivalent of political protesters, and the rise in hacktivist activity may be due in part to the growing importance of the Internet as a means of communication. Besides hackers who are in it for profit, there are hackers who break into systems to point out security flaws, and there are those who want to bring attention to a cause. The latter however, typically come in the form of virtual political activists who have adapted their methods of dissent into digital platforms, an act known as Hacktivism. Individuals proclaiming themselves as "hacktivists" often work secretly, sometimes operating in discreet groups while other times operating as individuals with cyber-world identities all consistent with the stated purpose of gaining public access and power in today's society (Sengupta, 2012).

BACKGROUND

Hacking originated in the 1960s via the Tech Model Railroad Club at Massachusetts Institute of Technology (Leeson & Coyne, 2005). These computer scientists were charged with "hacking" switch control systems of model trains, increasing their speed, making them more efficient. At this time, Artificial Intelligence was also introduced and brought about the first large mainframe computer system. Hacking became the solution in solving issues of the mainframe computer providing shortcuts and allowing the system to run quicker and simpler. Hacking in its infancy had little to do with malicious intent. The original goal was to advance computer usage and not impair it. Hacking then became a means of personal gain in the 1970s using phone systems. This activity was known a Phreaking, which is the act of carrying out illegal activity via the telephone system (Pavlik, 2017). Hacker gangs developed in the 1980s with the Milwaukee area's 414 gang. These noted individuals were able to access unauthorized outside computer systems and cause serious damage and disorder. The 414 gang is one of the first to be detained legally for their cyber-crimes (Leeson & Coyne, 2005). Consequently, in 1984, the government made it illegal to gain unofficial entry into a computer system.

Hacking is prevalent not only on computer systems, but the Internet as well. Cornell University was impacted by an Internet worm named Morris in 1988. The offender was sentenced to three years of probation (Leeson & Coyne, 2005). In the 1990s the pressing need to control the massive growth of the hacker occupation birthed the Federal Government to plan a series of raids in 14 cities known as "Operation Sundevil." The notion that the majority of hacking involves pranks by pubescent boys or inconsequential crime is outdated. Organized crime hackers seek more lucrative initiatives. Russian hackers also stole $10 million from Citibank, and the Federal Government responded in 1998 through the creation of the National Information Infrastructure Protection Center. Hacking overall is a world-wide phenomenon and is projected to become worse overtime. Denial-of-Service (DDoS) attacks that shutdown systems of enterprises such as Yahoo!, eBay, and Amazon, cost the global economy billions in lost revenue. Hacking comprises of breaching passwords, generating e-mail bombs, DDoS intrusions, scripting and circulating viruses, worms, and Trojans, screening prohibited intellectually property, URL redirection, and web defacement (Leeson & Coyne, 2005).

Cyberattacks have gained national and international attention. In 2008, a group named Anonymous opened a number of cyberattacks to assist a range of political and social issues. The focus and purpose of the group spans from commercial to government to religious organizations. On January 7th, 2013, Anonymous issued a "We the People" request asking the White House (United States of America) to acknowledge dispersed denial-of-service (DDoS) incidents as an endorsed form of demonstration safe-guarded by the First Amendment of the United States Constitution (Li, 2013). Alongside Anonymous' position, commentators posit that Hacktivism expands to digital civil disobedience, even if success is