Chapter 16
Cyber-Attacks, Retaliation and Risk:
Legal and Technical Implications for Nation-States and Private Entities

Cameron S. D. Brown
Australian National University, Australia

ABSTRACT

This chapter examines legal and technical issues that arise when considering strategic retaliatory countermeasures to cyber-attacks. Implications connected with endorsing techniques of active defense for nation-states are viewed alongside challenges faced by private entities. Proactive avenues for tackling cyber-security threats are evaluated and shortcomings within the international system of governance are analyzed. Retributive justice as a legal and philosophical concept is viewed through the lens of customary international law pertaining to use of force and self-defense. Difficulties in adapting rules governing kinetic warfare to instances of cyber-conflict are elucidated. The danger of executing counterstrikes for private entities is explained with reference to cross-border dilemmas, conflict of laws, and risks stemming from civil, criminal, and also administrative liability. Protocols for safeguarding anonymity are observed and the problem of attribution is illustrated. Costs and benefits associated with adopting methods of active defense are presented and solutions to avoid accountability failure are recommended.

INTRODUCTION

For nation-states and private sector entities alike the interconnectivity and transnational reach of the Internet has facilitated a significant shift in economic wealth and power. The potential for cyber-attacks to target governments and corporations is a by-product of the anonymous and decentralized nature of the Internet (Lin, 2010). Computer hacking is a phenomenon that challenges existing notions of warfare, espionage, competitive intelligence (Kovacich, Jones & Luzwick, 2002), and also of crime (Yasin, 1998). The capacity of nation-states and private entities to protect themselves from cyber-attacks is constantly in flux as new attack methods are developed and reactive defenses are devised. Ultimately, strategic

DOI: 10.4018/978-1-5225-7912-0.ch016

advantage lies with the aggressor and the defensive posture adopted by those under siege typically leads to initial loss or damage before vulnerabilities are patched and armored ("Microsoft Security," 2015). Between 2013 and 2015 the average cost of a data breach is estimated to have increased by 23% (Ponemon Institute, 2015).

Cyber-security may be seen to function within an adversary-based paradigm where defensive security innovators and consumers are pitted against persistent rogue attackers and highly organized operatives. In this cat-and-mouse struggle, defense cannot afford a single mistake, whilst those in offence have the advantage of time and need only achieve success on one occasion. In the digital domain, even minor breaches can be critical as data is syphoned out of governmental agencies and departments of defense, and intellectual property is pilfered from corporate networks. The vulnerability of nation-states and their critical infrastructure to Distributed Denial of Service Attacks (DDoS) also raises issues concerning to use of force, self-defense, and rules of engagement. Cyber-threats have become diversified and often comprise multi-stage attacks that use an assortment of attack tools that target a wide spectrum of technologies. The adversarial nature of this digital skirmish is multidimensional and the whole concept of retaliation is laden with risk, posing unique legal and technical problems.

The continuum of potential methods for seeking cyber-retribution is variously labelled 'hacking back', 'striking back', 'active defense', 'offensive retaliation', 'countermeasures', 'counteroffensives', 'counterattacks', 'counterstrikes' or 'forcible cyber-defense', amongst others. This chapter examines the legality and technical feasibility of conducting counteroffensives for both nation-states and private entities. The implications of retaliation for the public and private sphere are analyzed from a legal and operational standpoint. Uncertainties and risks are evaluated across a range of contexts, including the potential for reprisals to escalate conflict and intensify crisis situations.

BACKGROUND

In the wake of recent reports of persistent cyber-exploitation globally, coupled with disclosures concerning unabashed national cyber-surveillance programs (Gorman & Valentino-Devries, 2013), the issue of cyber-defense and retaliation is very topical (Limnell, 2014; Sorcher, 2015; Yadron, 2015). Following the lead of corporate giants like Google (Nakashima, 2013; Richmond, 2010) it seems nation-states and the private sector may resort to the use of forcible cyber-defense following instances of cyber-harm and transnational transgressions via the Internet (Kesan & Hayes, 2012; Messerschmidt, 2013). In 2010, Google announced that a group purportedly identified as the 'Elderwood Gang' (also known as the 'Beijing Group') infiltrated the Company's network, and breached at least thirty other corporations based in the United States (Cha & Nakashima, 2014; Clayton, 2012). The attackers utilized malware known as Hydraq, also referred to as Aurora, in combination with a zero-day exploit (O'Gorman & McDonald, 2012). Nicknamed "Operation Aurora", the cyber-attack was allegedly traced to servers located at two Chinese educational institutions (Kurtz, 2010; "Protecting your critical assets," 2010). Once identified, it is reported that Google launched a counteroffensive targeting the perceived attack source (Sanger & Markoff, 2010).

Unlike passive defense mechanisms, which endeavor to identify or prevent cyber-attacks before harm occurs, active defense aims to proactively retaliate by striking-back against intruders using counter-intelligence, deception, disruption, and destructive means (Kesan & Majuca, 2010). Hacking back encompasses everything from intrusive collection of intelligence to convict culprits, through to launch-