Chapter 7
A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine:
Exemplifying the Evolution of Internet-Supported Warfare

Kenneth J. Boyte
Cabrillo College, USA

ABSTRACT

This comparative international case study of cyber warfare provides a context for considering the evolution of cyber technologies as elements of hybrid warfare capable of creating confusion, disrupting communications, and impacting physical infrastructure (such as power grids and satellite-based communications and weapons systems). Expanding an unpublished paper recognized by the ASIS Foundation in its 2012 international student writing competition concerning global security, which compared the cyberattacks against Estonia in 2007 and the United States in 2012, this study re-examines and updates the original data in a broader analysis that primarily includes the cyberattacks against Ukraine during the 2013-2015 conflict, but also considers other incidents on the timeline of digitization. The study shows how cyber warfare, first reported in the 1990s, has become an integral component of war today for both state and non-state actors who use zombies and robot armies to penetrate national boundaries and firewalls via satellites.

INTRODUCTION

In the context of information operations and related cyber espionage (Geers, 2015), as well as what Russian General Valery Gerasimov (2016) described as hybrid warfare, this comparative international case study provides an open-source analysis of cyberattacks against three modern and Internet-reliant democracies: Estonia in 2007 (Kozlowski, 2014), the United States in 2012 (Goldman, 2012), and Ukraine during the 2013-2015 conflict (Woehrel, 2015). The analysis is important for historically evaluating the threats that

DOI: 10.4018/978-1-5225-7912-0.ch007

cyber warfare now and in the future may pose to international security (Maigre, 2015; Shackelford, 2009) in light of evolving technologies and doctrines of warfare that have made cyberattacks an integral part of modern warfare (Bachmann & Gunneriusson, 2015) and enabled the Internet to manipulate critical infrastructure (Geers, 2015; Lee, Assante, & Conway, 2016; Szoldra, 2016; Volz, 2016).

Describing this threat to material things and human life, the United States Department of Homeland Security (USDHS) (2016) stated, "[T]here are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on [national security]." These sectors include: energy, defense, nuclear, transportation, food and agriculture, emergency services, communication, chemical, dams, finance, healthcare, information technology, commercial facilities, and government facilities (USDHS, 2016). NATO has defined the term similarly, stating, "It is our critical infrastructure that makes modern society possible" (Kerigan-Kyro, 2014, p. 1).

Now capable of inflicting considerable material damage to critically important systems of government, communications, and daily life (Tucker, 2014), the Internet as a platform of cyber warfare also has broadened the battlefield to include state and non-state actors (Geers, 2015), who "increasingly rely on technological means to execute their operations utilizing cyber capabilities… against the IT infrastructure of a target" (Bachmann & Gunneriusson, 2015, p. 198). Recognizing this threat, since 2011, the United States Department of Defense has considered cyberspace a domain of war similar to the physical dimensions of air, land, and sea (Brownlee, 2015), despite a lack of national and international consensus defining cyber war, cyber warfare, and related terms (Gervais, 2012; Hathaway, et al., 2012; NATO, n.d.). Generally, hybrid warfare refers to the combined utilization of both kinetic and non-kinetic forms of combat, including economic sanctions, energy blockades, information warfare, and cyberattacks (Gerasimov, 2016; Maigre, 2015; McDermott, 2014; U.S. Army Special Operations Command, 2015).

Dedicated or distributed denial of service (DDoS) attacks—one common form of cyber warfare that dominated the cyberattacks against Estonia, the United States, and Ukraine—use automated spamming techniques to overload and shut down websites, disrupt communication flows and power grids, and otherwise compromise computer networks now connected to the 'Internet of Things' (Evron, 2008; Gilbert, 2014; Smith, 2016). These types of computer attacks—which target Domain Name Servers (DNS), "the phone books or roadmaps of the Internet" (Smith, 2016)—typically involve zombie armies of 'hijacked computers' that hackers control through the use of downloaded malware, defined by Anagnostopoulos, et al. (2013) as malicious software unknowingly downloaded "that compromises devices connected to the Internet. After that, the herder of the botnet is able to command the infected computers (bots) to carry out whatever pernicious action they desire" (p. 3). In cyberspeak, a zombie is a single hijacked personal computer, while a botnet is a network of hijacked computers numbering from hundreds of thousands to millions, described by Evron (2008) as "online robot networks" (pp. 123-124) that "exploit millions of compromised computers" (p. 126).

Numerous nations have been targeted by DDoS attacks, including Argentina (Tomlinson, 2013), Armenia (BBC News, 2012b), Canada (Wingrove & Quinn, 2015), China (Bruno, 2008), Finland (O'Dwyer, 2016), France (Vaughan-Nichols, 2014), Germany (Rosencrance, 2001), Georgia (Hollis, 2011), Great Britain (BBC News, 2016), Holland (Chirgwin, 2012), Italy (Cluley, 2011), Iran (Coleman, 2012), Israel (Estrin, 2016), Kyrgyzstan (Kozlowski, 2014), Kazakhstan (Windrem, 2016), Pakistan (Awan & Memon, 2016; Awan et al., 2016), Saudi Arabia (Geers, 2011), South Korea (The Globe and Mail, 2011), and Sri Lanka (Easttom & Taylor, 2011), where in 1998 the separatist group the Tamil Tigers launched the first reported DDoS attacks by non-state actors against a government's computer system (Easttom & Taylor,