Active Countermeasures as Retribution for Cyber Attacks

Celine Cuevas
February 5, 2015

Prof. Joan Feigenbaum,
Dept. of Computer Science, Yale University

Introduction

A cyber attack is defined as “any action taken to undermine the functions of a computer network for a political or national security purpose.”¹ In other words, it is a cyber crime – an illegal act committed using a computer-based means – committed by a state actor, rather than an individual, for a nationalist or political purpose. Some examples of cyber attacks include Distributed Denial of Service (DDOS) attacks, semantic attacks and secure computer network infiltration.

Some cyber attacks can be interpreted under the laws governing conduct in the course of war – known as jus in bello – or when they constitute an armed attack, under traditional jus ad bellum. However, many examples of cyber attacks do not rise to the level of an armed attack justifying self-defense as they have no direct physical consequences.

Instead, it has been proposed that these types of cyber attacks can be examined through other legal frameworks. One such framework is the international law of countermeasures, which regulates how states may respond to international law violations that do not meet such a threshold. The law indicates that an injured state may respond

---

with a reciprocal act, and in the context of cyber attacks, this retribution is interpreted as an “active defense” to attempt to disable the source of the attack.

Designing an appropriate active countermeasure poses a number of practical challenges including identifying the attacker, creating an effective countermeasure that causes the attacker to cease its unlawful behavior, and targeting only the actor that perpetuated the attack.

Thus, this project will focus on exploring active countermeasures as a response to cyber attacks. I plan to succinctly summarize our current state of computer and network security to explain the potential and variety of cyber attacks. I then plan to propose whether active countermeasures, under our current legal landscape, are an adequate way to prevent and/or respond to them.

**Milestones**

- Gain a background knowledge of:
  - Computer and network security
  - Cyber attacks
  - Current laws concerning war and how they’ve recently been interpreted to acknowledge cyber attacks
  - Examples of active countermeasures and other methods of retribution against cyber attacks, and their successes and/or failures

- Propose:
  - Whether active countermeasures are an appropriate, adequate and/or feasible response to cyber attacks
  - Examples of active countermeasures or other legally justified retributions to cyber attacks, or argue altogether that these are not the best way to respond to such attacks

- Write up final paper
Background Readings

Sample readings to gain background knowledge include:

  - Chapter 1: Is There a Security Problem in Computing?
  - Chapter 2: Elementary Cryptography
  - Chapter 3: Program Security
  - Chapter 7: Security in Networks

- Scholarly legal articles by Oona Hathaway including:

Deliverables

The deliverable for this project will be a final paper, approximately 15 pages in length, that focuses on active countermeasures in response to cyber attacks. The first portion will give an overview of computer and network security, cyber attacks and active countermeasures, and the laws that have been used to interpret and justify retribution against such attacks. The second portion of the paper will serve as a proposal, either arguing that active countermeasures are an adequate and legally justified response to cyber attacks and proposing some examples of effective countermeasures, or that they are not an ideal form of retribution and instead suggesting alternatives.