Striking Back in Response to Cyber-Attacks

Team members: Drew Hoskins, Yi-Kai Liu, Anil Relkuntwar

In recent years several people have proposed methods of counter-attacking or "striking back" in response to a cyber-attack. Strike-backs are useful in stopping an attack as it occurs (for instance, stopping a denial-of-service attack, or slowing the spread of a worm). They are an attractive option in cases where traditional law enforcement has been ineffective, such as international phishing scams and cyber-extortion, because a strike back can quickly cross national boundaries. However, the actual value of strike-backs in the real world is not well understood. Also, strike-backs have an uncertain legal standing. Intruding into other people's systems is illegal, though in some circumstances it might be justified as an act of self-defense. If the strike-back crosses national boundaries, it raises questions about state sovereignty. Better guidelines are needed to address these issues.

Here is a brief outline of our ideas:

I. General questions:
A. How do we define "offensive counter-attack?" Is a cyber-investigation followed by legal action included in this? How about posing as a hacker to get information?
B. What can a counter-attack accomplish? Are there ways to reduce the collateral damage?
C. Why do we need this capability? In what situations is this an appropriate response? (Resort to warfare in cases where traditional law enforcement methods are ineffective?) Also, can offense be more cost-effective than defense?

II. What kinds of offensive measures are available? Are they feasible? What are the effects of these attacks? Examples:
A. Trace-back to identify the source of an attack (requires hacking into third-party machines)
B. White worms to neutralize compromised hosts, e.g., Tim Mullen's strikeback idea
C. DDOS for retaliation (is this ever a good idea?)
D. Other possibilities...?

III. Legal issues
A. Are there legal principles or precedents (e.g., self-defense) that could justify a counter-attack? (Also, military ideas such as rules of engagement, proportional response?)
B. Legal framework: When is a counter-attack permissible? Who is allowed to do it? Do they need to collect evidence or document their actions?
C. See Karnow's notes

Division of labor: We are still figuring this out--it will probably depend on what specific attack techniques we decide to study. One of us (Yi-Kai) may focus on the legal issues.