Legal & Ethical Considerations of Offensive Cyber-Operations?

David Willson
Titan Info Security Group, LLC

Ben Tomhave
LockPath, Inc.

Session ID: STAR-304
Session Classification: General Interest

RSACONFERENCE2012

David Willson, Attorney at Law

U.S. ARMY
ARMY STRONG.

REVERENTIA LEGUM

LONG ISLAND UNIVERSITY

JUDGE ADVOCATE GENERAL'S CORPS

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON DC

TOURO LAW
Touro College Jacob D. Fuchsberg Law Center

(CISSP)®

ISSA™
Information Systems Security Association
The Global Voice of the Information Security Profession

INFRAGARD
PARTNERSHIP FOR PROTECTION

Ben Tomhave

LUTHER COLLEGE

THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON DC

(CISSP)®

ISSA™

Information Systems Security Association

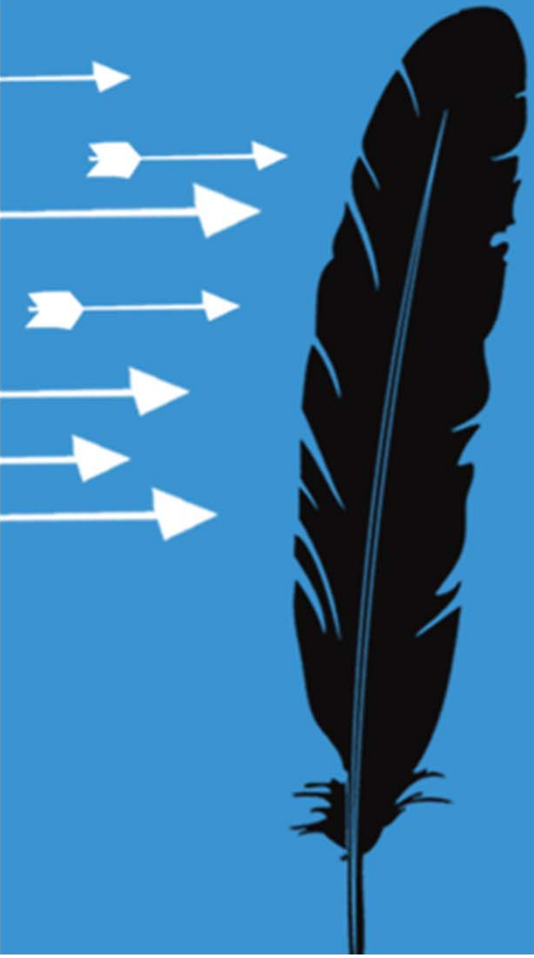
The Global Voice of the Information Security Profession

OWASP

The Open Web Application Security Project

Agenda

- Threat - A Brief Overview
- Recent Events
- What is…
  - …a Cyber Weapon?
  - …an Offensive Cyber Response?
- Nation-State Response
- Corporate Response
- Pushing the Envelope



The Setup

Abstract

Nations have the right - and in some cases obligation - to use cyberspace tools in an offensive manner to defend themselves.

What about businesses, do they also have this right?

This session will explore the legal and ethical issues surrounding the use of offensive cyberspace by both nations and corporations.

Learning Objectives

- Legal and ethical issues nations consider (at least the US) and corporations should consider when deciding whether or not to employ the use of offensive cyberspace.
- Recent attacks on nations and corporations.
- The decision and thought process the US uses to work through legal/ethical issues prior to using offensive cyberspace.
- Possible thought/decision process for corporations contemplating offensive cyberspace.
- Exposure to views from both sides of the spectrum on the legal and ethical use of offensive cyberspace.

Threat – A Brief Overview

Malicious Code

A Case Example

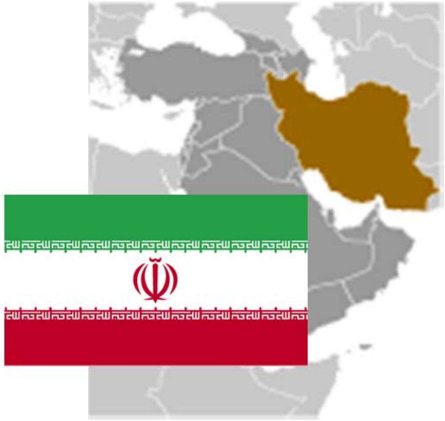
What can/should the US do?

Image Source: http://www.flickr.com/photos/23905174@N00/1594411528/sizes/m/in/photostream/

Recent Events – High Profile

citi®

RSA SECURITY™



STRATFOR

JPMorgan

Google

Zappos.com POWERED by SERVICE®

LOCKHEED MARTIN

Recent Events – Not-so-High Profile

Definitions

What Is a Cyber Weapon?

Cyber weapons pose a significant threat to a nation's ability to protect itself and to wage war. *They include:*

- angle reflectors
- autonomous mobile cyber weapons
- backdoors in commonly used software
- defense shields against electronic attack
- electronic countermeasures
- false-target generators
- info-blockades
- worms
- sniffing
- spyware
- malware
- botnets
- key-loggers
- IP spoofing
- infrared decoys
- Trojan horses
- viruses
- rootkits
- spamming
- transient electromagnetic devices

Source: www.technolytics.com/Dept_of_Cyber_Defense.pdf

What Is a Cyber Weapon?

Note: *there are at least two other cyber weapons* that are under development and classified.

There are two key characteristics of a cyber weapon: versatility and propagation.

Image Source: http://www.flickr.com/photos/1observatory/5206755959/sizes/m/in/photostream/

NATO Conf. on Cyber Conflict

Definition 9. An information technology weapon, or shorter – IT weapon, is an information technology-based system (consisting of hardware, software and communication medium) that is designed to damage the structure or operations of some other system(s).

NATO Conf. on Cyber Conflict

Definition 10. A Cyber Weapon is an information technology-based system that is designed to damage the structure or operations of some other information technology-based system(s).

The Bottom Line

A cyber weapon is: any tech tool used to deny, degrade, disrupt or destroy another's network, computer, or system, etc.

A hammer is a hammer and a weapon – it all depends on how it is used.

Image Source: http://www.flickr.com/photos/thenationalguard/3586724830/sizes/s/in/photostream/

What is an Offensive Cyber Response?

“Cyber Attack”

A hostile act using computer or related networks and/or systems, and intended to disrupt and/or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves - for instance, attacks on computer systems which are intended to degrade or destroy infrastructure of C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery.

Source: DoD Intelligence Glossary

What is an Offensive Cyber Response?

“Offensive Cyberspace Operations”

Activities that, through the use of cyberspace, actively gather information from computers, information systems, or networks, or manipulate, disrupt, deny, degrade, or destroy targeted computers, information systems, or networks. This definition includes Cyber Operational Preparation of the Environment (C-OPE), Offensive Counter-Cyber (OCC), cyber attack, and related electronic attack and space control negation.

Source: DoD Intelligence Glossary

Use of Force

Nation-State Use of Offensive Cyber Weapons

Legal Issues: pretty straight forward.

Issue of neutrality: Does the launching of an cyber attack from one nation to another violate the neutrality of all the nations it traverses?

Ethical Issues: Is it ethical to launch/use an offensive cyber weapon?

What if the cyber weapon is a virus or worm that is uncontrollable?

Can anyone say STUXNET?

Image Sources: http://www.flickr.com/photos/pincharrata/3672926041/sizes/t/in/photostream/
http://www.flickr.com/photos/paul_everett82/2833551397/sizes/s/in/photostream/

Corporate Response - Legal Issues

The Main Issue – CFAA (in the US) and similar laws:

"Whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby . . . (must cause harm)"

Can we all agree **it is illegal to gain unauthorized access** to a computer we do not own or have not been given access to?

Image Source: http://www.flickr.com/photos/ensh/6204837462/sizes/s/in/photostream/

Corporate Response - Legal Issues (p2)

Continuing the botnet theme…

What if you could put code on the "phone-home" function of the bot in your network and – when it talks to its CnC server – block the communication path essentially cutting the bot off from its master?

Is It Legal?

Is It Self-Defense?

Image Source: http://www.flickr.com/photos/caguard/5812224134/sizes/s/in/photostream/

Corporate Response - Questions

Have you gained unauthorized access?

Did you intentionally gain unauthorized access?

What if the botnet was disrupted for some other reason and the code you embedded in the bot never went anywhere. *Was the intent still there?*

What if – other than blocking the communication path for this bot – you *did not cause* any negative consequences for this CnC server?

Image Source: http://www.flickr.com/photos/anhonorablegerman/5626502674/sizes/m/in/photostream/

Corporate Response – Assumptions – Pre-requisites

You do not know where the CnC server is or who owns it!

The bot in your network is persistent and causing damage or stealing data and, despite all attempts, you have not been able to rid yourself of it!

You contacted LE and there was nothing they could do at this time!

Illegal or Self-Defense ?

Image Source: http://www.flickr.com/photos/bill_lim/2710187651/sizes/m/in/photostream/

Ethical Issues

Is placing embedded code on a bot ethical?

Is it ethical to do this knowing it will access someone else’s network and potentially have an impact on their system?

Is it ethical for Ad companies and others to put cookies, adware, spiders, add-ons, spam, etc., on our machines?

Is use of a virus or worm unethical simply due to their uncontrollable nature?

Is it unethical to use a mirror to bounce a DDoS attack back on the originating site?

Is it ethical for a social site to (MyLife.com) so post your name, address, past locations?

Image Source: http://www.flickr.com/photos/11304375@N07/2769553173/sizes/m/in/photostream/

Pushing the Envelope

Legal Issues: We know we can, but should we be pushing into the legal gray areas to defend ourselves?

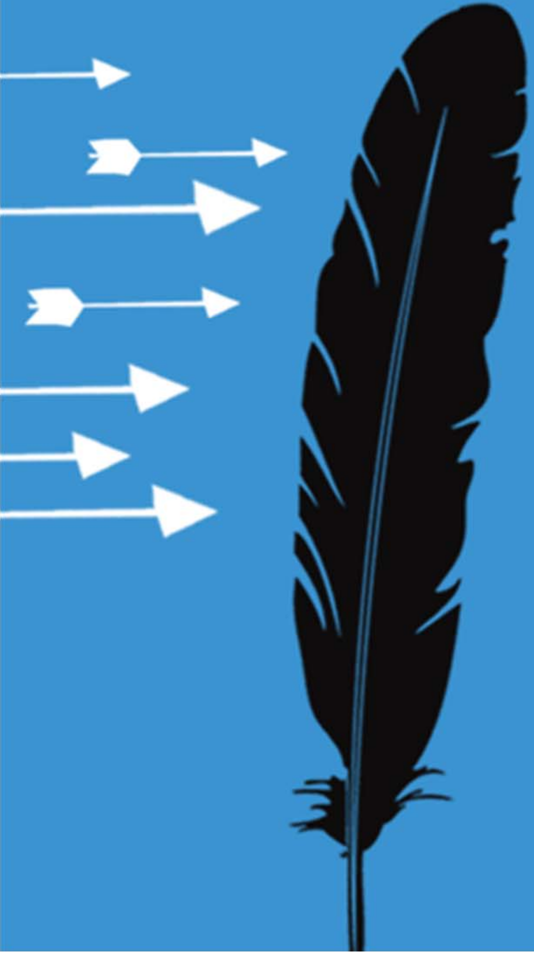
Gen. Alexander, US CYBERCOM:

"Active Defense" = "actively engaging in protecting your networks"

"What's reasonable and proportional?"

Ethical Issues: Is it ethical to push into the gray areas? Have we basically tied our own hands legally when it comes to cyberspace?

Image Source: http://www.flickr.com/photos/familymwr/5548053540/sizes/s/in/photostream/



Application

How to Apply This Talk

The first three months:

- Understand your context
- Know your rights & responsibilities

Within the year:

- Establish your own legal stance
- Codify your stance in policy
- Tool-up and train as appropriate

*** BLUF: Keep the discussion going!**

Image Source: http://www.flickr.com/photos/mcgraths/3248483447/sizes/m/in/photostream/

Questions??

Thank You!

David Willson
Attorney at Law
david@titaninfosecuritygroup.com
719-648-4176

Ben Tomhave
@falconsview
ben.tomhave@lockpath.com
www.lockpath.com

Image Source: http://www.flickr.com/photos/fun_flying/340406105/sizes/m/in/photostream/