Legal Aspects of Full Spectrum Computer Network (Active) Defense Black hat USA 2013
Agenda

- Disclaimer
- Errata
- Self Defense in Physical World
- Applying Self Defense to Computer Network Defense
  - Technology
  - Pen Testing/Red Teaming
  - Intelligence/Open Source
  - IA and Training/Polices
  - Information Control
  - Active Defense
    - Deception
    - Operating on The “Net”
I have an active defense scenario.
Disclaimer
Disclaimer - aka the fine print

- Joint Ethics Regulation
- Views are those of the speaker
- I’m here in personal capacity
- Don’t represent view of government
- Disclaimer required at beginning of presentation.
- All material - unclassified
U.S. Law
And Computer
Network Operations
We the People

Article I

Section 1. All legislative Powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives.

Section 2. The Congress shall assemble at least once in every year, and such meeting shall begin at the first Monday in December, unless they shall by law appoint a different day.

Section 3. When the Congress shall be in session the Secretary of State shall transmi...
History

1787 - Constitution Convention
1991 - Computer Crime Unit
1995 - CCIPS and the CTC Program
2000 - First CHIP Unit: NDCA
2001 - 10 CHIP Units Announced
2004 - The CHIP Network
2006 - DAG Memo: Duties defined
2007 - USAM 9-50.000: CHIP Guidance
2008 - Total 25 CHIP Units

Oh yeah, 1986 CFAA
Definition of Special Skills

- Special skill – a skill not possessed by members of the general public and usually requiring substantial education, training or licensing.

- Examples – pilots, lawyers, doctors, accountants, chemists and demolition experts.
- Not necessary to have formal education or training
- Skills can be acquired through experience or self-tutelage.

- Critical question is whether the skill set elevates to a level of knowledge and proficiency that eclipses that possessed by the general public.

In re Innovatio IP Ventures, LLC Patent Litigation & ECPA


- Patent Owners of wireless Internet technology
- Sue commercial users of wireless Internet technology
- Alleging by making wireless Internet available to customers or using it to manage internal processes, users infringed various claims of 17 patents.
- Plaintiff Innovatio has sued numerous hotels, coffee shops, restaurants, supermarkets, and other commercial users of wireless internet technology located throughout the United States (collectively, the “Wireless Network Users”).

- Decision
  - Data packets sent over unencrypted wireless networks
  - Readily accessible to general public using basic equipment
  - Patent owner's proposed protocol for sniffing accessed only communications sent over unencrypted networks available to general public using packet capture adapters
  - Falls under exception to Wiretap Act “electronic communication is readily accessible to the general public.”
  - Evidence obtained using protocol admissible at patent infringement trial with proper foundation. 18 U.S.C.A. § 2511(2)(g)(i).
In re Innovatio IP Ventures, LLC Patent Litigation & ECPA


Innovatio intercepting Wi–Fi communications
- Riverbed AirPcap Nx packet capture adapter (only $698.00)
- Software (wireshark) available for download for free.
- Laptop, software, packet capture adapter-
  - Any member of general public within range of an unencrypted Wi–Fi network can intercept.
  - Many Wi–Fi networks provided by commercial establishments are unencrypted and open to such interference from anyone with the right equipment.

In light of the ease of “sniffing” Wi–Fi networks, the court concludes that the communications sent on an unencrypted Wi–Fi network are readily accessible to the general public.
The public's lack of awareness of the ease with which unencrypted Wi–Fi communications can be intercepted by a third party is, however, irrelevant to a determination of whether those communications are “readily accessible to the general public.” 18 U.S.C. 2511(2)(g)(i)
Legal Aspects of Full Spectrum Computer Network (Active) Defense
Black Hat topic
Is it Relevant??
Support Grows to Let Cybertheft Victims 'Hack Back'

By CHRISTOPHER M. MATTHEWS

As companies weather a spate of high-profile computer attacks, support is growing for an option that for now is probably illegal: fighting back.

The Justice Department has long held that if a company accesses another party's computer network without permission, for whatever purpose, it is breaking the law.

A commission led by Dennis C. Blair, President Barack Obama's first director of national intelligence, and Jon M. Huntsman Jr., the former U.S. ambassador to China, said last month that "without damaging the intruder's own network, companies that experience cybertheft ought to be able to retrieve their electronic files or prevent the exploitation of their stolen information."
Defending life and liberty and protecting property, twenty-one state constitutions expressly tell us, are constitutional rights, generally inalienable, though in some constitutions merely inherent or natural and God-given.

Self Defense - History

- Self-defense and defense of property are long-recognized legal doctrines, traditionally protected by the common law.
Common Law doctrine – Trespass to Chattel

- Recover actual damages suffered due to impairment of or loss of use of property.

- May use reasonable force to protect possession against even harmless interference.

- The law favors prevention over post-trespass recovery, as it is permissible to use reasonable force to retain possession of chattel but not to recover it after possession has been lost.

Self Defense - History

- Right to exclude people from one’s personal property is not unlimited.

- Self-defense of personal property one must prove
  - in a place right to be
  - acted without fault
  - used reasonable force
  - reasonably believed was necessary
  - to immediately prevent or terminate other person's trespass or interference with property lawfully in his possession.

The common-law right to protect property has long generally excluded the right to use force deadly to humans.

Self Defense - History

- Common Law Doctrine – Trespass to Chattel
  - May use reasonable force to protect possessions against even harmless interference.
  - Prevention over post-trespass recovery

- Self-defense of personal property
  - in a place right to be
  - acted without fault
  - used reasonable force
  - reasonably believed was necessary
  - to immediately prevent or terminate other person's trespass or interference with property lawfully in his possession.
Full Spectrum Computer Network Defense

- Building the Case of Reasonableness
  - Defense of Property
  - Conduct constituting an offense is justified if:
    - (1) an aggressor unjustifiably threatens the property of another, and
    - (2) the actor engages in conduct harmful to the aggressor:
      - (a) when and to the extent necessary to protect the property,
      - (b) that is reasonable in relation to the harm threatened.
Full Spectrum Computer Network Defense

- Building the Case of Reasonableness
  - Measures Done to Secure and Defend
    - Technology
    - Intelligence/Situational Awareness
    - IA/Policies/Training
    - Information Control
    - Active Defense
      - Deception
      - Recovery Operations
    - “Stop the Pain”
Full Spectrum Computer Network Defense

- Building the Case of Reasonableness
  - What was missing from previous slide and goes directly to reasonableness

- PREVIOUS & ONGOING COORDINATION WITH LAW ENFORCEMENT AGENCIES
Full Spectrum Computer Network Defense

- Building the Case of Reasonableness
- Measures Done to Secure and Defend
  - Technology
  - Intelligence/Situational Awareness
  - IA/Policies/Training
  - Information Control
- Active Defense
  - Deception
  - Recovery Operations
  - "Stop the Pain"
Building the Case of Reasonableness

Why?

- Attempting to convince DOJ (any prosecutorial office) NOT to prosecute for your actions.

- Worse Scenario – Attempting to convince Judge/Jury that your actions were extremely reasonable and therefore self defense to your CFAA charges.
Full Spectrum Computer Network Defense

- Building the Case of Reasonableness
  - Reality & Practicality
    - DOJ taking a hard stance with “active defense”
    - Requirement for self-defense/necessity
      - No other lawful means (i.e. LEA)
        - All means/remedies exhausted
          - LEA
          - Civil lawsuits
Building the Case of Reasonableness

Although it may be tempting to do so (especially if the attack is ongoing), the company should not take any offensive measures on its own, such as “hacking back” into the attacker’s computer—even if such measures could in theory be characterized as “defensive.” Doing so may be illegal, regardless of the motive. Further, as most attacks are launched from compromised systems of unwitting third parties, “hacking back” can damage the system of another innocent party.
Full Spectrum Computer Network Defense

- Building the Case of Reasonableness
  - Measures Done to Secure and Defend
    - Technology
    - Intelligence/Situational Awareness
    - IA/Policies/Training
    - Information Control
    - Active Defense
      - Deception
      - Recovery Operations
      - “Stop the Pain”
Technology

- Firewalls
- Intrusion Detection Systems
- Intrusion Prevention Systems
- Real Time Network Awareness
- SSL Proxy
- Logging/Monitoring
  - Host (accounts, processes, services)
  - Networks (flows, connections, stat)
- Honeypots/Honeynets/Honeytokens
To Legally Intercept Communications, Exception to Wiretap Act Must Apply

- Party to the Communication or Consent of a Party to the Communication

- Provider Exception (System Protection)
Consent

Where there is a legitimate expectation of privacy, consent provides an exception to the warrant and probable cause requirement.

A computer log-on banner, workplace policy, or user agreement may constitute user consent to a search. See United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 1999)
Wiretap Statute: Rights or Property Exception


A provider “may intercept or disclose communications on its own machines “in the normal course of employment while engaged in any activity which is a necessary incident to . . . the protection of the rights or property of the provider of that service.”

Generally speaking, the rights or property exception allows tailored monitoring necessary to protect computer system from harm. See U.S. v McLaren, 957 F. Supp 215, 219 (M.D. Fla. 1997).
Generally speaking, the rights or property exception allows tailored monitoring necessary to protect computer system from harm.

Technology

- Intellectual Property
- Trade Secrets
- Research & Development
- The Crown Jewels
- Air Gap
Beacons

18 USC § 3121 - GENERAL PROHIBITION ON PEN REGISTER AND TRAP AND TRACE DEVICE USE; EXCEPTION

This preliminary release may be subject to further revision before it is released again as a final version. As with other online versions of the Code, the U.S. Code Classification Tables should be consulted for the latest laws affecting the Code. Those using the USCPrelim should verify the text against the printed slip laws available from GPO (Government Printing Office), the laws as shown on THOMAS (a legislative service of the Library of Congress), and the final version of the Code when it becomes available.

Current through Pub. L. 112-123. (See Public Laws for the current Congress.)

(a) In General.— Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) Exception.— The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service—

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or (3) where the consent of the user of that service has been obtained.

(c) Limitation.— A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.

(d) Penalty.— Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.
Beacons

It makes sense that a person using a communication service should be able to consent to another person monitoring addressing information associated with her communications. For example, a person receiving threats over the Internet should be able to consent to the government collecting addressing information that identifies the source of those threats. And indeed, the Pen Register statute does contain an exception for use of a pen/trap device with the consent of the user. But there is an issue with the consent provision: it may only allow the use of the pen/trap device by a provider of electronic communication service, not the user or some other party designated by the user. So in the Internet threats example, the provider is the ISP, not the victim herself or the government. If the provider is unwilling or unable to implement the pen/trap device, even with the user’s consent, the statute may prohibit the United States from assisting the victim. Clarifying the Pen Register statute on this point may be appropriate.
Pen Testing/Red Teaming

- Spear Phishing


- National system of trademark registration

- Protects owners of federally registered marks against the use of similar marks

  - if such use is likely to result in consumer confusion, or
  - if the dilution of a famous mark is likely to occur.
Pen Testing/Red Teaming

- Spear Phishing
- Dilution

The use of a mark or trade name in commerce sufficiently similar to a famous mark that by association it reduces, or is likely to reduce, the public’s perception that the famous mark signifies something unique, singular or particular.
Intelligence/Situational Awareness

- Open Source Intelligence
  - US-CERT
  - Commercial Intelligence Provider
- Active Business Intelligence
  - Competitive Intelligence v. Economic Espionage

- Protects proprietary economic information making some trade secret theft a crimes.

- Congress enacted for “a systematic approach to the problem of economic espionage.”

- Designed to reflect the importance "intangible assets" and like trade secrets in the "high-technology, information age."

- Section 1831 Economic Espionage
- Section 1832 Theft of Trade Secrets
  - Obtaining trade secret without authorization
  - Copy, altered or transmitted a trade secret without authorization
  - Received a trade secret knowing information was stolen or obtained without authorization.
Intelligence/Situational Awareness


- See Douglas Nemec and Kristen Voorhees, Recent amendment to the Economic Espionage Act extends protection against misappropriation, found at http://newsandinsight.thomsonreuters.com/Legal/Insight/2013/02_February/Recent_amendment_to_the_Economic Espionage_Act_extends_protection_against_misappropriation/
Intelligence/Situational Awareness

  - Broad and applies to more than just intentional theft.
  - Can be a significant hazard for companies that legitimately receive the confidential information of another company.
  - Some lawful methods for gathering business intelligence or “research and development leads” may in fact constitute acts of trade secret misappropriation.
  - Trade secret can be virtually any type of information, including combinations of public information.

- Douglas Nemec and Kristen Voorhees, Recent amendment to the Economic Espionage Act extends protection against misappropriation, found at http://newsandinsight.thomsonreuters.com/Legal/Insight/2013/02_-February/Recent_amendment_to_the_Economic_Espionage_Act Extends_protection_against_misappropriation/
Whether the information was a trade secret is the crucial element that separates lawful from unlawful conduct. Possession of open-source or readily ascertainable information for the benefit of a foreign government is clearly not espionage. The essence of economic espionage is the misappropriation of trade secret information for the benefit of a foreign government.

Intelligence/Situational Awareness

Intelligence/Situational Awareness

- Firms routinely gather publicly available or “open-source” information about rivals a lawful practice known as competitive intelligence.

- Competitive intelligence is the ethic and lawful application of industry and research expertise to analyze publicly available information on rivals and to produce actionable intelligence that supports informed and strategic business decisions.

Intelligence/Situational Awareness

- Desired Information
  - Research Plans
  - R&D Data
  - Product Design
  - Marketing Strategies
  - Cost Structures & Pricing Strategies

Intelligence/Situational Awareness

- Common competitive intelligence methods
  - Data mining
  - Patent tracking
  - Psychological modeling of rival executive
  - Trade shows
  - Monitoring mass media
  - Conversations with a rival’s customers, partners, and employees.

Intelligence/Situational Awareness

- Competitive intelligence does not connote misappropriation by theft, deception, or otherwise of proprietary information or trade secrets.

- Focus on open source public information.
  - Shareholders reports
  - Advertising
  - Sales literature
  - Press releases, news stories, published interviews

Intelligence/Situational Awareness

- Competitive intelligence that raises ethical questions
  - Appropriating documents misplaced by rivals
    - (iPhone?)
  - Overhearing rival executives discussing strategy
    - (Misplaced Trust & Third Party Doctrine)
  - Hiring employees away from rivals
  - “Dumpster diving” in rival’s trash receptacles.

Intelligence/Situational Awareness

Methods of Economic Espionage
- Electronic eavesdropping
- Surveillance of rival executives and scientists
- Social Engineering
- Bribing employees or vendors
- Planting “moles” in rival firms
- Hacking and stealing computers
- Cybertheft of data
- Outright stealing trade secrets in documentary, electronic, and other formats.

Intelligence/Situational Awareness

- Methods of Economic Espionage
  - Electronic eavesdropping
  - Surveillance of rival executives and scientists
  - Social Engineering
  - Bribing employees or vendors
  - Planting “moles” in rival firms
  - Hacking and stealing computers
  - Cybertheft of data
- Outright stealing trade secrets in documentary, electronic, and other formats.

Intelligence/Situational Awareness

- *United States v. Aleynikov*, 676 F.3d. 71 (2d Cir (SDNY) Apr. 11, 2012)
  - Sergey Aleynikov, was a former computer programmer and vice president in Equities at Goldman Sachs.
  - Responsible for developing computer programs used in the bank’s high-frequency trading (HFT) system.
  - HFT system used statistical algorithms to analyze past trades and market developments.
  - System was proprietary information and protected by various security measures to keep it secret.
  - Sergey makes $400K, highest paid of 25 programmers in his group.
  - Hired at competitor at over $1M
Intelligence/Situational Awareness

- *United States v. Aleynikov*, 676 F.3d. 71 (2d Cir (SDNY) Apr. 11, 2012)
  - Last day of employment
  - Just before going away party
  - Aleynikov encrypted and uploaded to a server in Germany 500,000 lines of source code.
  - After upload, deleted the encryption program and history of his computer commands.
  - Later downloads source code from the German server to his home computer in the United States, flew to Chicago, Illinois, and brought the source code with him to a meeting with a Goldman Sachs competitor.
Intelligence/Situational Awareness

- *United States v. Aleynikov*, 676 F.3d. 71 (2d Cir (SDNY)) Apr. 11, 2012
  - Defendant was convicted of stealing and transferring proprietary computer source code of his employer's in violation of National Stolen Property Act (NSPA) and Economic Espionage Act (EEA)
  - Aleynikov appealed arguing that Section 1832(a) only applies to trade secrets “relating to tangible products actually sold, licensed or otherwise distributed.” *The source code, he argued, was never intended to be placed in interstate or foreign commerce.*
United States v. Aleynikov, 676 F.3d. 71 (2d Cir (SDNY) Apr. 11, 2012

Defendant was convicted of stealing and transferring proprietary computer source code of his employer's in violation of National Stolen Property Act (NSPA) and Economic Espionage Act (EEA)

Aleynikov appealed arguing that Section 1832(a) only applies to trade secrets “relating to tangible products actually sold, licensed or otherwise distributed.” The source code, he argued, was never intended to be placed in interstate or foreign commerce.

The Court of Appeals held that: computer source code did not constitute stolen “goods,” “wares,” or “merchandise” within meaning of NSPA and defendant's theft of source code did not violate EEA.
Obama Signs Theft of Trade Secrets Clarification Act into Law


As previously discussed on TSI, the law (which passed unanimously in the House and Senate) was passed in response to the Second Circuit's controversial decision in United States v. Aleynikov. The Clarification Act broadens the EEA's reach by striking the relevant language in § 1832(a) (i.e. "or included in a product that is produced for or placed in") and inserting "a product or service used in or intended for use in". 
IA Policies/Training

- IA Training
- Banners
- User Agreements
- Annually/Semi/Quarterly
- Enforcement
- Employee discipline for violating?
Information Control

- Access lists
- Encryption
- DRM
- Electronic Mail Control
Active Defense
Deception
Active Defense
Deception
& The SEC
Form 10-K

The federal securities laws require publicly traded companies to disclose information on an ongoing basis. For example, domestic issuers (other than small business issuers) must submit annual reports on Form 10-K, quarterly reports on Form 10-Q, and current reports on Form 8-K for a number of specified events and must comply with a variety of other disclosure requirements.

The annual report on Form 10-K provides a comprehensive overview of the company's business and financial condition and includes audited financial statements. Although similarly named, the annual report on Form 10-K is distinct from the "annual report to shareholders," which a company must send to its shareholders when it holds an annual meeting to elect directors.

Historically, Form 10-K had to be filed with the SEC within 90 days after the end of the company's fiscal year. However, in September 2002, the SEC approved a Final Rule that changed the deadlines for Form 10-K and Form 10-Q for "accelerated filers" -- meaning issuers that have a public float of at least $75 million, that have been subject to the Exchange Act's reporting requirements for at least 12 calendar months, that previously have filed at least one annual report, and that are not eligible to file their quarterly and annual reports on Forms 10-QSB and 10-KSB. These shortened deadlines will be phased in over time.

In December 2005, the SEC voted to adopt amendments that create a new category of "large accelerated filers" that includes companies with a public float of $700 million or more. The amendments also redefine "accelerated filers" as companies that have at least $75 million, but less than $700 million, of public float.
Section 21(a) of the Exchange Act authorizes the Commission to investigate violations of the federal securities laws, and, in its discretion, “to publish information concerning any such violations.”

Active Defense - Deception

- Regulation full disclosure requires companies to distribute material information in a manner reasonably designed to get that information out to the general public broadly and non-exclusively. It is intended to ensure that all investors have the ability to gain access to material information at the same time.

Active Defense - Deception

- A company makes public disclosure when it distributes information “through a recognized channel of distribution.”
  - So if deception
    - Documents on internal computer systems
    - No intent of being made public
    - Stolen
    - Documents leaked to media
    - Company has not made a public disclosure
    - SEC violations or an investigation?
Active Defense

- Deception Examples
  - RFPs
  - Bid Preparation
  - Blue Prints/Designs
    - Minor Defects
    - Major Defects - Cause Harm?
- Business Plans/Financial Records
- Mergers & Acquisitions
  - Liability to Third Parties Mentioned in Deception Documents
Certificate of Completion
of the
Star Fleet
Kobayashi Maru Exercise

This certificate is awarded to

for the completion of the Kobayashi Maru Command Training Exercise. This exercise is a test of character, there are no winners. You have shown the resolve and courage to knowingly enter a no-win situation in order to uphold the values and basic tenants of the United Federation of Planets.

MINHUF, PATRICK N. HENK
Training Simulation Officer

UNITED FEDERATION OF PLANETS

Certification Authority
SAN FRANCISCO • MMCLXI
Active Defense – Recovery Operations

- Recovery Operations
- An Example of Clark's Law
Active Defense – Recovery Operations

Intruder

FTP Server

Innocent Third Party

Victim

Intruder
Intruder

FTP Server

Innocent Third Party

Victim

Issues

1. Logs
   a. Third Party
   b. FTP Server
   c. Third Party
Active Defense – Recovery Operations

Intruder

FTP Server

Innocent Third Party

Victim

Innocent Third Party
Active Defense – Recovery Operations

1. Closed FTP Server
   a. Login information from your logs.
Active Defense – Recovery Operations

- Recovery Operations
- Assume good CNE
Active Defense – Stop the Pain

- The Part with a lot of audience participation
- So what do you want to do
- What “pain” do you need to stop?
- DDoS, ????
- C&C
- bots ????
Active Defense – Stop the Pain

- “Stop the Pain”
- Good CNE
Active Defense – Stop the Pain

If I fry the guy who is attacking me - Who is going to sue me, the guy attacking me!??!
Active Defense

For instance, the commission argues that U.S. laws should let American owners of intellectual property recover or render inoperable any IP that’s stolen over the Internet. Such laws would allow companies to consider a broader use of "meta-tagging," "beaconing" and "watermarking" tools to digitally mark any files containing proprietary data.

The tools would alert companies to the theft of a protected file, and could help identify where it was stored by the cybercriminals. Such tools would also let IP owners render a stolen file inaccessible or lock down an authorized user's computer. Such measures do not violate existing Internet laws and could reduce some of the incentive for hackers to steal IP, the commission said.

The IP Commission's report also cited what it said are growing calls to create a more "permissive environment" that allows American companies to launch offensive cyber actions against IP thieves. The offensives could help companies retrieve stolen information, alter it within an intruder's computer or network, or destroy it.
"Additional measures go further, including photographing the hacker using his own system's camera, implanting malware in the hacker's network, or even physically disabling or destroying the hacker's own computer or network," the report said.

The IP Commission acknowledges that cyber retribution measures are not currently legal under U.S. law, and should not be considered today and acknowledged that "An action against a hacker designed to recover a stolen information file or to degrade or damage the computer system of a hacker might degrade or damage the computer or network systems of an innocent third party."
Hack Back

  - TRO
    - “[T]here are special needs, including to protect the public and to perform community caretaking functions, that are beyond the normal need for law enforcement and make the warrant and probable-cause requirement of the Fourth Amendment impracticable”
    - “the requested TRO is both minimally intrusive and reasonable under the Fourth Amendment.”
Hack Back

- The Coreflood botnet
  - Five C & C servers seized
  - 29 domain names used to communicate with the C & C servers
- If C & C servers do not respond, the existing Coreflood malware continues to run on the victim’s computer, collecting personal and financial information. TRO authorizes government to respond to requests from infected computers in the United States with a command that temporarily stops the malware from running on the infected computer.