CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

Current Threat to the U.S. from Cyber Espionage & Cyberterrorism

Presented by SSA Elvis Chan
FBI San Francisco

Overall Classification: UNCLASSIFIED//FOR OFFICIAL USE ONLY

FBI Priorities - Post 9/11

- Counterterrorism
- Foreign Counterintelligence
- **Cyber**
- Public Corruption
- Civil Rights
- Criminal Enterprises
- White Collar Crime
- Violent Crime

The Cyber Threat

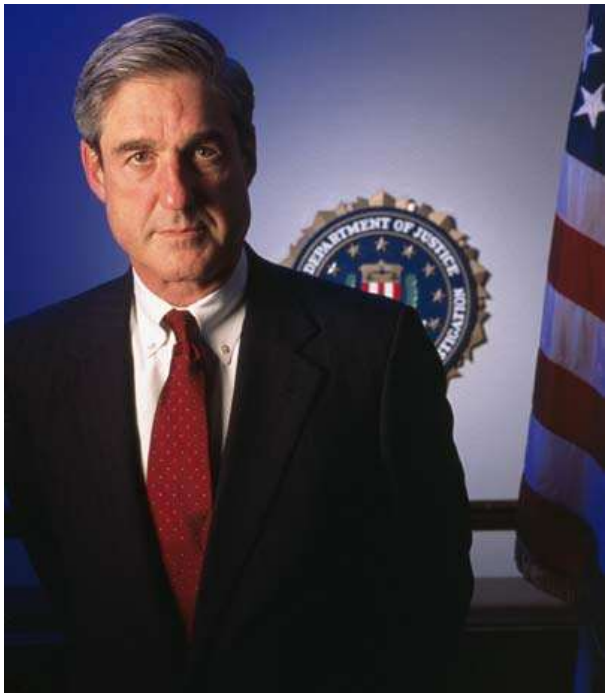
"America's economic prosperity in the 21st century will depend on cyber security…"

President Barack Obama
May 29, 2009

The Cyber Threat

"Terrorism does remain the FBI's top priority, but in the not too distant future we anticipate that the cyber threat will pose the greatest threat to our country."

FBI Director Robert S. Mueller III
March 1, 2012



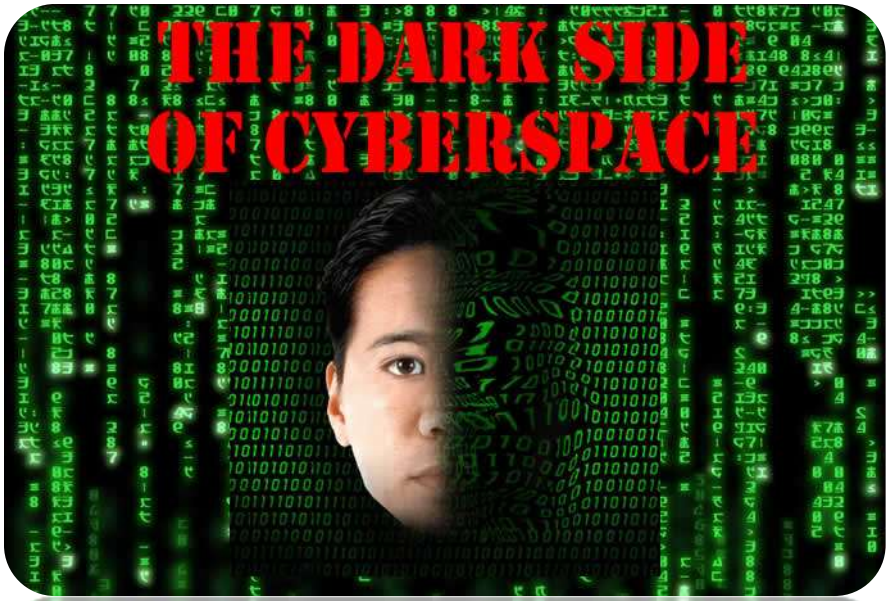
The Cyber Threat

"I don't see cyber as a thing, I see it as a way. As a vector."

FBI Director James B. Comey
January 7, 2015

Cyber Threats

- Hacktivism
- Cyber Crime
- **Cyber Espionage**
- Cyberterrorism
- Cyber Warfare



Cyber Espionage Definition

What is cyber espionage?

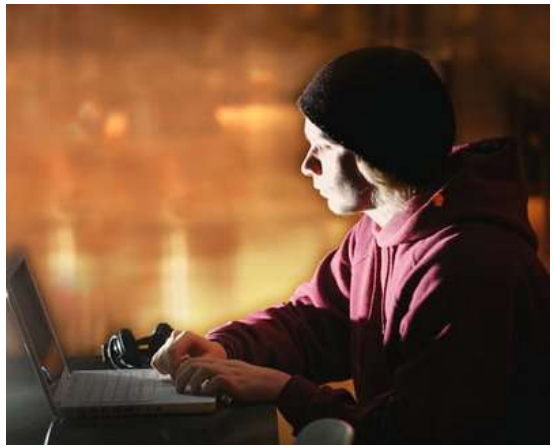
- *Cyber espionage is the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary, or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks, or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware.*

-Wikipedia

Cyber Espionage – What?

What is going on?

- State sponsored adversaries are pursuing sensitive U.S. information and proprietary technologies.
- U.S. company networks house this information and may be vulnerable to exploitation.



Cyber Espionage – Who?

Who is doing it?

"**Chinese actors** are the world's most active & persistent perpetrators of economic espionage. U.S. private sector firms and cyber security specialists have reported an onslaught of computer network intrusions that have originated in **China**."

"The governments of **China** and **Russia** will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace."

Foreign Spies Stealing US Economic Secrets in Cyberspace
Office of the Director of National Intelligence
Published: October 2011
http://www.dni.gov/reports/20111103_report_fecie.pdf

Cyber Espionage – How?

How do they do it? The exploitation of trust:

- The trusted incoming e-mail.
- The publicly available trusted web site of appropriate business interest.
- The download of trusted code from a trusted and authorized vendor.
- The trusted protocols for data transfer.
- The inherent trust of the internal corporate network.
- The trusted external client server.

Cyber Espionage – Why?

Why do they do it?

- Meet intelligence collection requirements
- Acquire information for advantage
  - Military
  - Economic
  - Political
- Target key individuals with access
- Create future opportunities

Cyber Espionage – Case Study #1

- November 2001, two Chinese nationals were arrested at SFO just before boarding a flight to Shanghai.
- Thousands of proprietary documents and electronic media from NEC, Sun, Transmeta, and Trident were seized.

Cyber Espionage – Case Study #2

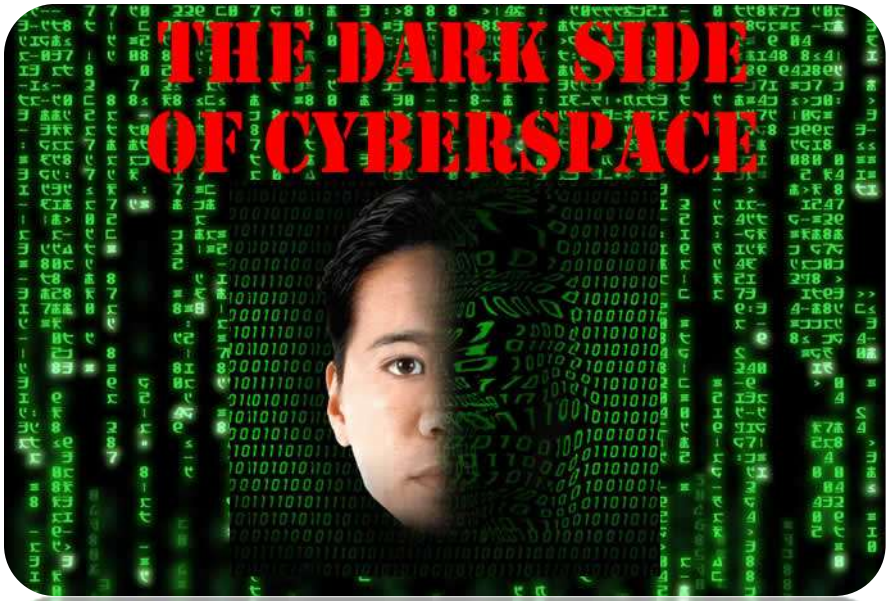
- On May 19, 2014, the Dept. of Justice announced a first-of-its-kind cyber espionage case against Chinese military officials.
- Five PLA officials were charged with hacking into U.S. companies to steal trade secrets.

Cyber Espionage – Case Study #3

- In October 2014, security researchers identify a new sophisticated Chinese cyber espionage group dubbed “Axiom.”
- Axiom targets the U.S., other Western countries, and Chinese dissidents inside and outside of China.
- Active for at least six years:
  - Hikit malware provides advanced persistent threat.
  - Maintenance cycles to switch out malware on victim machines.

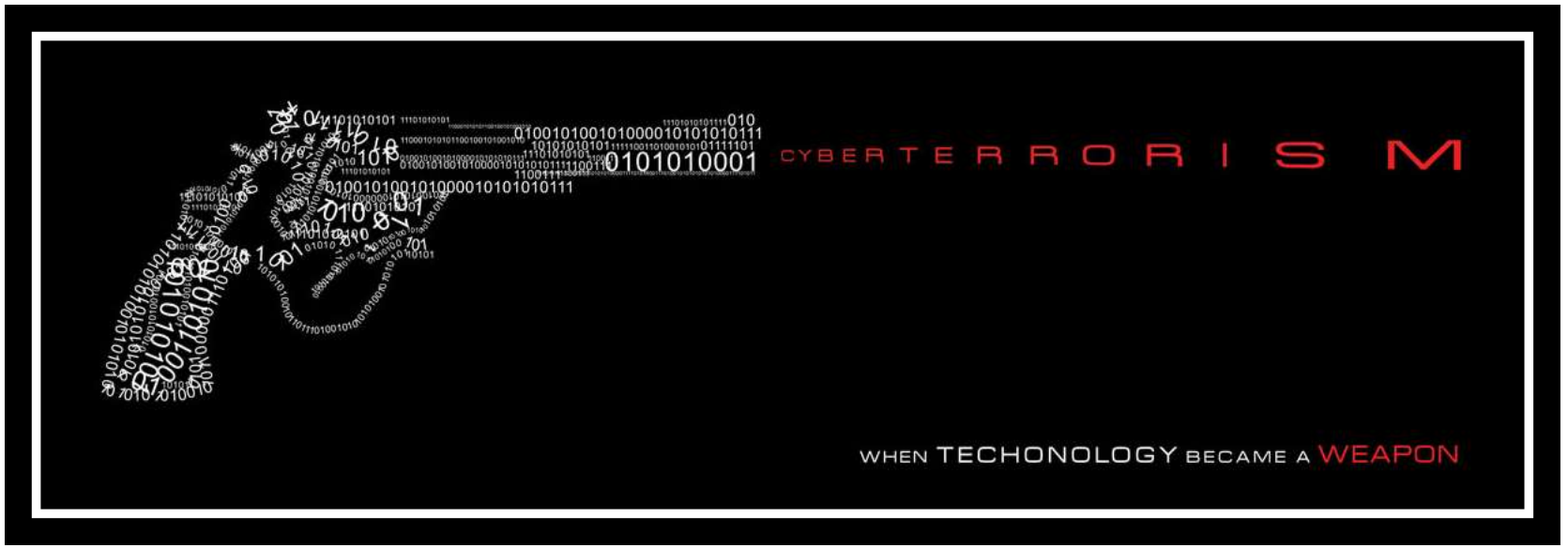
Cyber Threats

- Hacktivism
- Cyber Crime
- Cyber Espionage
- **Cyberterrorism**
- Cyber Warfare



Cyberterrorism – What?

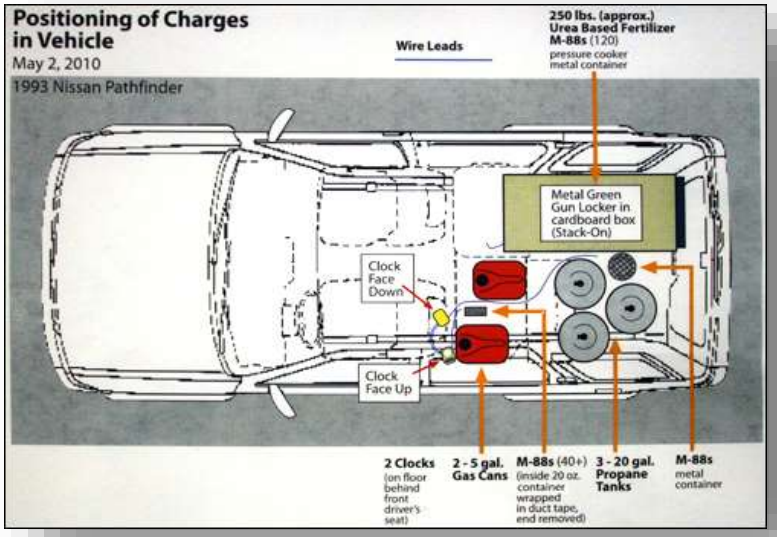
- What is cyberterrorism?
- Terrorist Use of the Internet vs. Cyberterrorism



Terrorist Use of the Internet Example

Times Square Bombing

- Faisal Shahzad
  - Public Web Cameras
  - File-sharing websites
  - Proxy servers
  - Remote conferencing software
  - Claimed attack on YouTube



Cyberterrorism Definition

What is cyberterrorism?

- *Cyberterrorism is disruptive or destructive acts perpetrated against noncombatant targets at the direction, on behalf, or in support of a terrorist group or their ideology, through the use of computer network attack or exploitation. Such intrusions or attacks are intended to intimidate or coerce a government or population in furtherance of a social, political, ideological, or religious agenda by causing disruption, inducing fear, or undermining confidence.*

- FBI Definition

Cyberterrorism – Who?

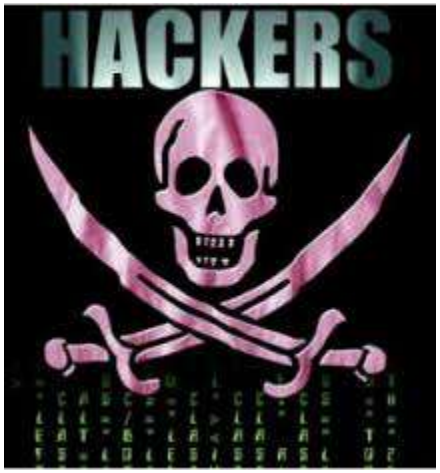
Who is conducting Cyberterrorism?

- Al-Qa'ida
- Islamic State of Iraq and Levant
- Hizballah
- Hamas
- Sympathizers

Cyberterrorism – How?

- Spearphishing
- Brute Force (Password crackers)
- Vulnerability Attacks (SQLI, XSS, etc.)
- Distributed Denial of Service (HOIC, LOIC, Lizard Stressor, etc.)

Cyberterrorism – Why?



- Propaganda or incite terror (website defacements)
- Fundraising (account hijacking, carding, etc.)
- Facilitation (Research/reconnaissance for kinetic attack)
- Disruptive acts to cause harm to life or damage to property

Cyberterrorism – Case Study #1

Mail Online

Home | U.K. Home | News | Sport | U.S. Showbiz | Femail | Health | Science | Money | Rig

News Home | Arts | Headlines | Pictures | Most read | News Board

British Muslim computer geek, son of diplomat, revealed as al Qaeda's top cyber terrorist

Last updated at 17:42

The world's most wanted cyber-jihadist

By Gordon Corera
BBC News security correspondent

When police raided a flat in West London in October 2005, they arrested a young man, originally from Morocco, called Younes Tsouli. They had no idea, at the time, just how significant he was.

From his bedroom on an ordinary road in Shepherds Bush, he had become one of the most notorious cyber-

Cyberterrorism – Case Study #1

- Compromised servers:
  - Stored beheading videos
  - Created proxy servers
  - Established communication channels
- Identity theft to acquire servers to host extremist sites
  - Created the “Youbombit” website
  - A “YouTube” for jihadists
- Collaborated with criminal hackers and extremists
  - Tested and utilized malware
- Was planning traditional kinetic attacks in Europe when he was arrested

Cyberterrorism – Case Study #2

- On 06 January 2015, CyberCaliphate, successfully took over the Twitter accounts of:
  - Albuquerque News Journal (Albuquerque, NM)
  - Mountain View Telegraph (Moriarty, NM)
  - WBOC News (Baltimore, Maryland).
- CyberCaliphate also hacked the websites of WBOC News and Mountain View Telegraph (a subsidiary of Albuquerque News Journal), and the Facebook account of Albuquerque News Journal.

Cyberterrorism – Case Study #2

- On 12 January 2015, CyberCaliphate obtained access to the Twitter and YouTube accounts for U.S. Central Command (CENTCOM).
- Hackers utilized the accounts to send the message, “American Soldiers, we are coming, watch your back. ISIS.”
- The hackers tweeted the location of purportedly stolen government files on pastebin.

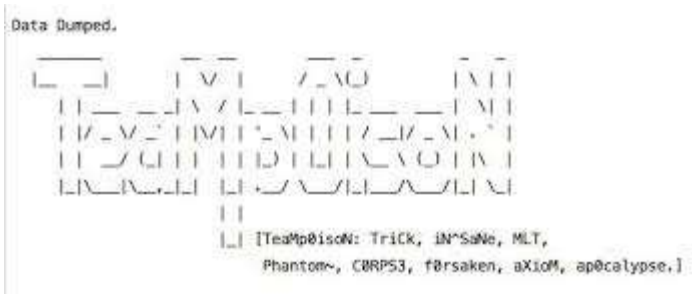
Cyberterrorism – Case Study #2

- On 10 February 2015, CyberCaliphate hacking group hacked the Twitter accounts of Newsweek and Latin Times, and the mobile message provider for WBOC News.
- CyberCaliphate tweeted from the Newsweek Twitter Account: “Bloody Valentine’s Day, #MichelleObama! We’re watching you, your girls, and your husband!”

Cyberterrorism – Case Study #3

Team Poison Member – Junaid Hussain aka “Trick”

- Arrested in July 2012 for denial of service attack on U.K. anti-terror hotline and doxing PM Tony Blair & family



Cyberterrorism – Case Study #3

Team Poison Member – Junaid Hussain aka “Trick”

- In August 2014, Hussain, while on parole, and his wife travel to Syria to join with ISIS. “Jihadi John” may have accompanied them.
- Hussain is now working on behalf of ISIS to set up and run Cyber Caliphate.

Cyber Trends

- Computer network operations by adversaries are becoming ubiquitous.
- Cyber adversaries will increasingly leverage social media for more tailored and targeted operations.
- The number of vulnerability points for adversaries to exploit will increase as people move to the “Internet of Things.”

Guidance - Prevention

What can I do to prevent a cyber attack?

- Establish Security Policies…then prioritize
- Support Established Security Policies
- Monitor and Analyze Network Traffic
- Assess Vulnerabilities
- Configure Systems for Security (may mean $$)
- Support Training for Employees

Guidance - Prevention

The To Do List Before a Cyber Attack

- Point of Contact for Legal, Technical and Project Management
- Legal Banner/Computer Use Agreement
- Employee Handbook/Corporate Policies
- Network Topography Maps
- Internal and External IP address and Host lists
- List of Network Devices (switches, routers, other devices)
- Incident Logs (Security, Host, IDS, Web, Database, Network)
- Archived Network Traffic
- Forensic Images of Compromised Hosts (live memory captures)
- Physical Access logs (video cameras, key cards, TFA devices)

Guidance – After the Attack

The To Do List After a Cyber Attack

- Follow your emergency plan and start protecting your data!
- Call the FBI.
- Preserve original media as evidence.
- Conduct analysis from a copy (if possible).
- Review ALL logs (DNS, Firewall, Proxy, System Event Logs).
- Contact ISP for additional logs and possible filtering.
- Begin damage assessment (including damage valuation).

What can the FBI do for you?

- Investigate
  - National and global reach
  - Combined technical skills and investigative experience
  - Long-term commitment of resources
- Forensics
  - Silicon Valley Regional Computer Forensics Laboratory (SVRCFL)
  - Keeps options open for your company
- Analyze Patterns and Links
- Bring national security concerns to the U.S. Intelligence Community

Investigation – A Case Study

Recent cyber attack at a local company

- FBI informed the company of possible computer intrusion.
- Company conducted internal investigation and found malicious software code, which was provided to FBI.
- FBI reverse engineered malware, identified attack structure, and developed indicators for dissemination.
- FBI provided indicators to company for its information security team to search logs for additional signs of compromise, and a scrubbed version to sector sharing group.
- Company can now look for other similar malicious code and help stop the loss of its intellectual property

What the FBI does not do

- Take over your systems.
- Repair your systems.
- Share proprietary information with competitors.
- Provide investigation-related information to the media or your shareholders.

FBI Tools

Title 18, United States Code

- Section 1029, Fraud in connection with access of devices
- Section 1030 (a)(5)(A)(i) Intentional Damage.
- 1030(a)(5)(A)(ii)Unauthorized Access, Reckless Damage
- 1030(a)(7) Extortion.
- 1831 Economic Espionage Act.
- 1832 Trade Secrets Act.

Way Forward

- ❑Cyber Warfare
- ❑Cyberterrorism
- ❑Cyber Espionage
- ❑Cyber Crime
- ❑Hacktivism

- ❑Investigation
- ❑Attribution
- ❑Disruption
- ❑Arrest, Seizure, Exploitation

- ❑Public/Private Partner Engagement
- ❑HUMINT
- ❑Surveillance
- ❑Digital Forensics

Way Forward

"***Maintaining a silence will not benefit you or your company in the long run***"

FBI Director Robert S. Mueller III March 1, 2012

FBI San Francisco Infragard Program Coordinator
SA Joy Mihara-Meer
510-808-8488
Yukiyo.Mihara-Meer@ic.fbi.gov

Questions


DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY
BRAVERY
INTEGRITY