Panel 4: Cyber Crime, Cyber Terrorism, and Cyber Espionage

CNU Symposium on Homeland Security & Defense
About Spectrum

16 Years in Business
250 employees worldwide

Defense Consulting
Cyber Security
System Integration
Test and Evaluation
Technical Data Management
Training
Cyber-Physical Systems

- Physical systems controlled by computers
- Examples include modern:
  - Automobiles
  - Aircraft
  - Ships and Submersibles
  - Buildings
  - Infrastructure
  - UxVs and Drones
  - Internet of Things

A Mission-Aware Cyber-Security Assessment is critical to developing a robust Resilience Strategy.

IN THE HEADLINES...

Cyberattack Physically Damages Iron Plant in Germany

Russian hackers suspected in attack that blacked out parts of Ukraine

ARMY Network Breached ... [through] Helicopter Simulator

Hacker Leaks S. Korea Nuke Plant Blueprints

From the Media

Cyber-physical attacks: Hacking a chemical plant

Hackers can now hitch a ride on car computers

Hackers Remotely Kill a Jeep on the Highway
Increasing Attack Sophistication

- Attack sophistication vs Intruder Technical Knowledge
- Tools:
  - “stealth” / advanced scanning techniques
  - binary encryption
  - GUI
  - automated probes/scans
  - www attacks
  - distributed attack tools
- Intruder Knowledge:
  - High
  - Low
- Attack Sophistication:
  - High
  - Low
- Attackers:
  - 1980
  - 1985
  - 1990
  - 1995
  - 2000
  - 2005
  - 2014

Geeks
Cottage Industry
Industrialization
Information from the Internet of Things:
We have gone beyond the decimal system

Today data scientist uses Yottabytes to describe how much government data the NSA or FBI have on people altogether. In the near future, Brontobyte will be the measurement to describe the type of sensor data that will be generated from the IoT (Internet of Things).

From: https://www.linkedin.com/pulse/iot-why-you-really-need-mapr-scale-brontobytes-geoff-clark
Some Concerns

• IT Security ≠ Cyber-Physical Security
• Security Objectives – Your Viewpoint Matters
• Scale of the Problem
• Speed of Industry vs Speed of Adversary
• IP Stacks – potential to inherit Internet-like issues
• Impact of IoT
• Impact Mobile (Vehicle) Networks
  – Impact of Autonomy or Semi-Autonomy
• The Rise of Attack Sophistication
Threat Agents

- **Organized Crime** – global and difficult to trace and prosecute
- **Cyber Warfare** (e.g., foreign governments) – stealing secrets, disruption
- **Hactivism and Cyber Terrorism** – inspired by ideology
- **Corporate Espionage** – stealing IP for products and transactions
Knowledge of your company’s exposure to attacks is fundamental in calculating your risk of vulnerability
Effective cyber security relies on a broad security program.
KPMG Cyber Security Framework – Summary

- Assess Current State
- Establish Your Strategy
- Develop Situational Awareness
- Build Intelligence Capability
- Deliver Results
- Ongoing Education & Communication
- Create Synergies with Related Activities
- Build Information Security into Business Processes
- Establish Executive & Board Support
- Implement Solutions
- Assess and Improve Capabilities
- Develop Your Team
- Police, Continually Assess & Improve
- Threat Analysis and Intrusion Detection
- Investigation
- Incident and Crisis Response
Cyber Maturity Assessment

- Leadership and Governance
- Operations and Technology
- Human Factors
- Information Risk Management
- Legal and Compliance
- Business Continuity and Crisis Management
Situational Awareness

- Know your business cycles well
- Know who your clients, suppliers & partners are
- Know what threats exist currently & where your gaps are
- Be open to your community
- Need to “share” versus need to know approach
- “Listen” for threats that will emerge
What is Required to Protect Against Cyber Threats?

A comprehensive review of preparedness against cyber attack

A rounded view of people, processes, physical, policy and technology factors need to be considered

Flexibility to assess level of cyber maturity on a site by site basis and at company level

Identification of best practice within the organization and comparative information against peer groups and competitors

Technical & cultural preparedness

Prioritized areas for remediation and a management action plan

Have you considered these in your strategic business planning?
Thank you.

Please share your thoughts with us. Your feedback is important.

Ian McPherson
Principal
Justice and Security Advisory
1 720 485 7276
ianmcpherson@kpmg.com
THE DRAGON IN THE MACHINE

A Case Study of Nation State Corporate Espionage
Presented By: J.D. Leasure, President/CEO
TABLE OF CONTENTS

- Factors That Influence State Sponsored Corporate Espionage
- Internal Vulnerabilities That Contribute To Penetration
- Undetected Exploitation: Disguising The Threat
- Incidence Response: Covert Cyber TSCM
- Multi-National Espionage Risks
Chinese Corporate Espionage is generally of two types:

1) Nation State Sponsored Espionage:
   Corporate Espionage sponsored by the Chinese government.

2) Privately Sponsored Corporate Espionage:
   Sponsored by Chinese corporations.

The focus of this presentation will be on Chinese Nation State sponsored espionage.
China is working feverishly to counteract its slowest GDP growth in recent years, and one of the ways it’s doing so is through the theft of American corporate secrets.

Rep. Mike Rogers, R-Mich., chairman of the House Intelligence Committee:
“There is a concerted effort by the government of China to get into the business of stealing economic secrets to put into use in China to compete against the U.S. economy.”

The Chinese are afraid of there is a ‘business gap’ that could hurt their economy now and in the future.

Source: http://www.cnbc.com/id/48099539/Chinese_Espionage_on_the_Rise_in_US_Experts_Warn
State Sponsored Espionage (Continued)

Adam Segal, a China Expert and Senior Fellow at the Council on Foreign Relations:

“While China's economic growth has been rapid and amazing over the last 30 years, the Chinese are afraid that they're going to get stuck in a technology trap. The Chinese feel that they have to rely on the West — and Japan — for critical technologies.”

According to Segal, China’s espionage is targeted toward the following industries because of their strategic importance:

- Green technologies
- New information technologies
- Biology
- High-end manufacturing

Source: http://www.cnbc.com/id/48099539/Chinese_Espionage_on_the_Rise_in_US_Experts_Warn
Jonathan Evans, director general of MI5:

"The extent of what is going on is astonishing. Industrial-scale processes involving many thousands of people lying behind both state-sponsored cyber espionage and organized cyber crime."

“Though Evans did not name any countries, ABC News has separately learned from sources that the U.K., the U.S. and several European allies have a robust discussion underway on how to counter cyber espionage by perhaps the most significant state operator -- China.”

“In contrast, the state players in the cyber sphere are those contesting for real geopolitical power – countries such as the U.S., China, Russia, Ukraine, Iran, Israel, some European nations and others who have the capabilities and aspirations to operate in the arena of cyber attack and defense on national infrastructures, in the espionage efforts to steal economically significant intellectual property, in investment to develop deterrence through credible offensive capability and in the effort to gain a seat at any future table on cyber arms control.”

State Sponsored Espionage (Continued)

CNBC Report: CYBER ESPIONAGE: THE CHINESE THREAT

http://youtu.be/Js52FjOsgPA
State Sponsored Espionage (Continued)

Suspected China Cyber Spying:

- **November 2006**: Chinese hackers attack the U.S. Naval War College computer infrastructure.
- **October 2007**: China is suspected as the source of a malicious email targeting 1,100 employees at the Oak Ridge National nuclear weapons lab.
- **January 2010**: Google says Chinese hackers breached its systems. Other companies attacked include Juniper Networks and Adobe Systems.
- **February 2011**: Computer security firm McAfee says in a report that it found evidence that Chinese hackers attacked five Western oil firms.
- **March 2011**: EMC Corp's security division, RSA says its systems were infiltrated using 'phishing' emails. Chinese hackers strongly suspected.

Source: [http://online.wsj.com/article/SB10001424052970204336104577094690893528130.html](http://online.wsj.com/article/SB10001424052970204336104577094690893528130.html)
According to Dan Stober - Author, A Convenient Spy: Wen Ho Lee and the Politics of Nuclear Espionage

- Chinese students and scientists are placed in US companies specifically to obtain trade secrets. Stober refers to the tactic as the “thousand grains of sand” approach where each person collects a small amount of information.

- China recruits US scientists to come to China, they wine and dine them, extracting information in the process. If they have relatives in China, they use leverage to get compliance, such as “we will give your grandmother a first floor apartment so she does not have to walk up to the third floor.”

Source: http://www.pbs.org/wgbh/pages/frontline/shows/spy/spies/different.html
Internal Vulnerabilities That Contribute To Penetration (Continued)

U.S.-China Economic and Security Review Commission by Northrop Grumman Corp:

“Activities attributed to state sponsored operators often appear to target data that is not easily monetized in underground criminal online auctions or markets, but highly valuable to foreign governments.”

“Highly technical defense engineering information, operational military data, or government policy analysis documents rarely if ever appear to be a priority for cybercriminal groups.”

Internal Vulnerabilities That Contribute To Penetration (Continued)

Office of the National Counterintelligence Executive, “FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE”, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011 (Continued)

Key Methods Employed By Chinese Cyber Spies:

- **Malicious software (malware):** presents opportunities for intelligence services and other actors to launch operations with limited resources and without developing unique tools that can be associated with them.

- **Hacker websites:** prevalent across the Internet, and tool sharing is common, causing intrusions by unrelated actors to exhibit similar technical characteristics.

- **Independent hackers:** FIS and other foreign entities have used them at times to augment their capabilities and act as proxies for intrusions, thereby providing plausible deniability.

- **Rerouting operations through other countries:** Many actors route operations through computers in third countries or physically operate from third countries to obscure the origin of their activity.

U.S. intelligence officials can identify different groups based on a variety of indicators, including:

- The type of cyber attack software they use
- Different Internet addresses they employ when stealing data
- How attacks are carried out against different targets

Source: http://online.wsj.com/article/SB10001424052970204336104577094690893528130.html
U.S. Pentagon Analyst:

“The news is disturbing. Chinese companies have the ability to remotely access the communication equipment sold to the United States and Western Countries. The revelation made by the open source intelligence company Lignet reinforces a lot of concerns about the possible presence of backdoors in communications devices that could allow the foreign government to disable the telecommunications infrastructure.

**China can shut down all the telecom infrastructures.**

“Transmitting devices may be exploited over time for purposes of cyber espionage in military and civilian, stealing technology, trade secrets and other confidential information.”

“While, on the domestic front the US Government, aware of its vulnerability, is moving defining and implementing cyber strategies aimed at strengthening its systems, the events of recent months have shown that relationships with contractors are the weakest link in the chain safety.”

Internal Vulnerabilities That Contribute To Penetration (Continued)

- A new China nation state sponsored cyber espionage threat has emerged:

  Extraction of information over the cellular network.
Undetected Exploitation: Disguising The Threat

- Plug & Play remote access devices.
- **NAC/802.1x Bypass.** In addition to supporting both 3G and Wireless connectivity, the plug & play devices can bypass virtually all NAC/802.1x/RADIUS implementations, providing a reverse shell backdoor and full connectivity to NAC-restricted networks.
Undetected Exploitation: Disguising The Threat

The Plug & Play device includes a full security auditing software suite and provides covert remote access over Ethernet, wireless, and 3G/GSM cell networks.
Undetected Exploitation: Disguising The Threat

Out-of-band SSH access over 3G/GSM cell networks, compatible with SIM cards from AT&T, Vodafone, Orange, and GSM carriers in over 160 countries.
Undetected Exploitation: Disguising The Threat

Onboard high-gain 802.11b/g/n wireless
Onboard high-gain Bluetooth (up to 1000')
Onboard dual-Ethernet
Fully functional 120/240v AC outlets!
Includes 16GB internal disk storage
Includes external 3G/GSM adapter
Undetected Exploitation: Disguising The Threat
Undetected Exploitation: Disguising The Threat

Richard Hale (One of the Pentagon's top cyber security officials)

"Everyone is at risk. Every business that is hooked to the Internet is vulnerable. It's like gravity; the threat is all around us."

Experts say, the key is understanding how systems can be hacked, and the steps to take to prevent it from happening.

Undetected Exploitation: Disguising The Threat (Continued)

Common Mechanisms of Disguising the Threat:

- Malicious code on a USB device
- Mimicking a trusted source (a customer, co-worker or even a family member) via email and entering your system when a photo or link is clicked.

Once they are in a system, they navigate laterally from computer to computer until they've gained the required credentials to access the entire network.

Undetected Exploitation: Disguising The Threat (Continued)

Common Methods of Disguising the Threat:


Advanced Persistent Threats (APTs): are modern, automated versions of traditional espionage. Operatives leverage and obfuscate cyber techniques, modeled after those in the physical world, in order to steal information and proprietary data in the cyber realm.

The Hackers Use “Spear Fishing” Techniques:

• Peer-to-peer networks (e.g. Linked In)
• Search engines
• Social networking (Facebook)
• Job sites

APTs are rarely detected and do not trigger any alerts!


**Targets Include:**

- Board members
- IT administrators
- Key executives
- Privileged users
- Supply chain
- Support staff

According to Deloitte Report, “Cyber Espionage - The harsh reality of advanced security Threats” (Continued):

**Tools Used Include:**

- Custom malware
- Packet capture tools
- Satellite imaging
- Targeted exploitation tools
- Wireless surveillance

According to Bloomberg News:

“The networks of at least 760 companies, research universities, Internet service providers and government agencies were hit over the last decade.”

Research in Motion Ltd.  Hewlett-Packard Co.
Boston Scientific Corp.  Google Inc.
Intel Corp.  Associated Computer Systems (A division of Xerox)
iBahn  Volkswagen AG
Yahoo! Inc.  Massachusetts Institute of Technology
Abbott Laboratories  The Italian Academic and Research Network
Wyeth (A division of Pfizer Inc.)  The California State University Network
Aerospace Corp.  Cypress Semiconductor Corp.

Case Study Of An Actual Nation State Corporate Espionage Incident:

- Company had reason to believe they were being collected against
- Company dispatches internal IT cyber security personnel twice, OCONUS
- IT cyber security team is unsuccessful detecting the threat or source on both occasions
- Meanwhile, company continues to leak proprietary/trade secret information on an emerging technology
- Internal corporate council is made aware of serious problem that continues
- Company sources third party cyber security consultants
- Cyber security consultants attempt to detect the threat or source unsuccessfully
- Cyber security consultants contact counter espionage specialist, ComSec LLC
Case Study Of An Actual Nation State Corporate Espionage Incident:

- After extensive consultation with the cyber security consultants, it is determined that there is a need to conduct a series of wireless communication tests with a goal of gaining an understanding of how wireless technologies may be involved in the leaks.
- In planning a covert wireless spectrum survey, ComSec designed an approach that would focus primarily on detecting and analyzing global, cellular, and consumer frequencies.
Case Study Of Actual Nation State Corporate Espionage:

- The target spectrum including all transmissions/emissions from 700 MHz to 4 GHz. Roughly all cellular, WiFi and blue tooth bands that are commonly utilized by mobile technology platform vendors and operators.

- Due to the import restraints imposed by the People’s Republic of China (PRC), TSCM capture and analysis equipment could not be used in this survey.
In order to detect and analyze these frequencies, ComSec utilized purpose built, dual purpose hardware and software that have been proven as effective tools capable of capturing a wide range of wireless communications.

Covert Cyber TSCM
Incidence Response: Covert Cyber TSCM  (Continued)

Getting The Wireless Collection Software in Country…
Incidence Response: Covert Cyber TSCM (Continued)

Safely & Securely..
A Highly Modified MacBook Pro Was Utilized For The Wireless Collection
Incidence Response: Covert Cyber TSCM (Continued)

A Modified Wheeled Briefcase Containing Radio Receiver and Antenna Array Were Utilized During The Wireless Collection.
Incidence Response: Covert Cyber TSCM (Continued)

RF Capture & Analysis Platform Testing Prior to PRC Assignment.
Incidence Response: Covert Cyber TSCM (Continued)

Assignment: PRC

SHANGHAI
Incidence Response: Covert Cyber TSCM (Continued)

Counterespionage Assignment: Conduct a series of wireless communications tests with the goal of gaining an understanding of how wireless technologies may be involved in the information security incidents that author’s team is responding to within client’s infrastructure.
Incidence Response: Covert Cyber TSCM (Continued)

Meeting with LN Asset (Local National) at Shanghai Waldorf Astoria
Incidence Response: Covert Cyber TSCM (Continued)

Old Shanghai Club – Room “1910”
Incidence Response: Covert Cyber TSCM (Continued)

Reconnaissance of Target Headquarters Building, Capture & Analysis of Local Wireless Signal Spectrum.
Incidence Response: Covert Cyber TSCM (Continued)

Shanghai Headquarters
Incidence Response: Covert Cyber TSCM (Continued)

Building Walk Through & Conference Room Setup
Unidentified cellular signal capture verified within target environment. Dead center within the local cellular band.
Incidence Response: Covert Cyber TSCM (Continued)

Cellular Repeater (Bi Directional Amplifier) located on third floor of building.
Incidense Response: Covert Cyber TSCM (Continued)

Cellular Log-Periodic Directional Antenna Located on 3rd Floor of Building.
Incidence Response: Covert Cyber TSCM (Continued)

Cellular Repeater Signal Capture Verified.
Incidence Response: Covert Cyber TSCM (Continued)

“Normal” Cell Phone Traffic - Cellular Signal Strength
Incidence Response: Covert Cyber TSCM (Continued)

Rouge Cellular Signal Enhanced Emanating From Server Room
Incidence Response: Covert Cyber TSCM (Continued)

Incidence Response: Covert Cyber TSCM (Continued)

High Power GSM Transmitter Located & Verified.
“ONE SPY IS WORTH A THOUSAND FOOT SOLDIERS…”

SUN TZU
MOSCOW RULES
FOR COUNTERESPIONAGE INVESTIGATIONS

• Assume that all LN’s are Hostile
• Assume that an approach by a non-LN is hostile until proven otherwise
• Assume that there is always hostile physical surveillance
• Assume that all communications are monitored by LN’s
• Assume that all enclosed areas are bugged
• Assume that all incoming and outgoing mail will be subject to examination
• Assume that anything left unattended will be subject to examination
• Assume that locks left unguarded or unprotected will be compromised
• Assume that simple traps will not deceive LN’s
• Assume that any guard can be recruited by LN’s or is himself an LN agent.
Conclusions

• Multi-national corporate espionage is a reality!
• Corporations have a responsibility to protect their intellectual property.
• There are U.S. laws in place to protect trade secret thefts, but corporations need to develop a plan to protect their own IP.
• It’s time to develop a corporate strategy to protect against corporate espionage!

COPYRIGHT © 2016 COMSEC LLC
Questions?