OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Cyber Threats to Supply Chains

Miguel Halling, National Counterintelligence Officer for Cyber

October 2014

THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE

- Reports to the Director of National Intelligence; however, the NCIX's authorities reach across the USG.

- The NCIX was created to serve as the head of national counterintelligence for the U.S. Government.

- The ONCIX mission includes carrying out and coordinating outreach programs, including to the US private sector.

CYBER ESPIONAGE

- Reports over the past decade estimate the loss from cyber espionage to be in the billions per year

- Proliferation of CNO tools by foreign companies and the underground market gives *less capable* actors means to conduct cyber (*and supply chain*) attacks

- Defense, Energy, Financial Services, Information Technology, Personally Identifiable Information, Communications, Critical Manufacturing, Engineering, Aerospace, Transportation, and Healthcare offer rich targets

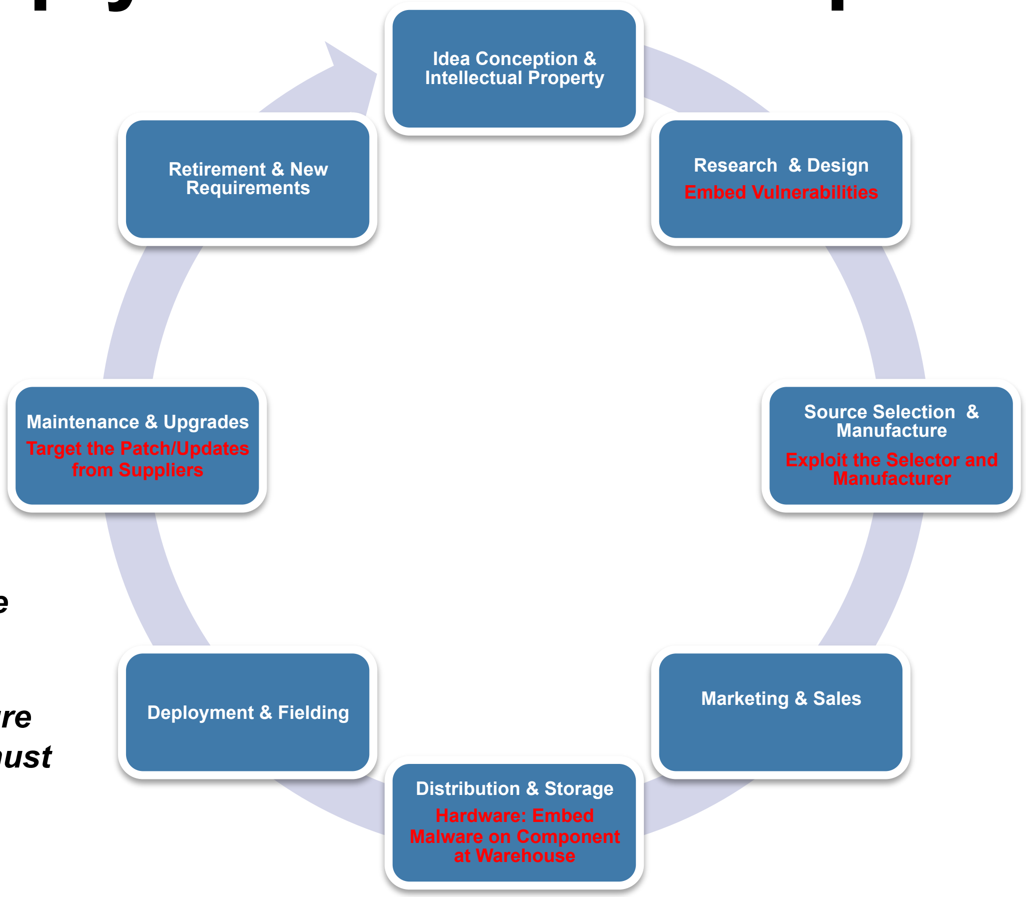
Where is the threat coming from?

- October 2011: ONCIX published *Foreign Spies Stealing US Secrets in Cyberspace*, which called out China and Russia.
- February 2013: Mandiant report exposed China’s cyber espionage capabilities with attribution.
- May 2013 Intellectual Property Commission Report estimated China is responsible for 50% to 80% of international IP theft.
- September 2013 Symantec Hidden Lynx report exposed East Asian hackers targeting supply chains using a custom driver application.
- June 2014 Symantec Dragonfly report exposed East European hackers targeting suppliers for US and European energy companies.
- Who else?

Information and Communications Technology (ICT) Industry a Prime Target

(U) The ICT industry is a target:

Anatomy of Cyber Enabled Supply Chain Access Operations



Idea Conception & Intellectual Property

Research & Design
Embed Vulnerabilities

Source Selection & Manufacture
Exploit the Selector and Manufacturer

Marketing & Sales

Distribution & Storage
Hardware: Embed Malware on Component at Warehouse

Deployment & Fielding

Maintenance & Upgrades
Target the Patch/Updates from Suppliers

Retirement & New Requirements

Unless operations are for disruptive purposes, as we build robust and enduring cyber security into our networks, current and future supply chain operations must have a cyber component.

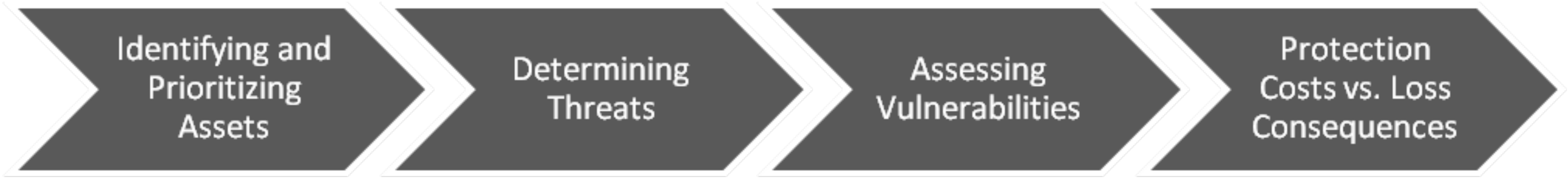
* Supply Chain Access Operations involve the modification of hardware or software with the purpose of enabling CNE.

USG Challenges and Successes

- Information Sharing
  - Good, bad, and ugly
- Volume, Volume, and Volume
  - Where are the Resources?
- Criticality Analysis
  - Both good and bad
- Supply Chain Views
  - Counterintelligence
  - Engineers

Risk Management

- 100% protection cannot be achieved, regardless of expenditures
- Risk Management is the foundation of Corporate Counterintelligence programs



Identifying and Prioritizing Assets

Determining Threats

Assessing Vulnerabilities

Protection Costs vs. Loss Consequences

SUPPLY CHAIN RISKS

CASE EXAMPLES

(U) East Asian Cyber Attacks on Supply – Hidden Lynx & TrapX

(U) East European Cyber Attack – Dragonfly

(U) Information Security Company #1

(U) Data Virtualization Company

(U) Information Security Company #2

(U) Information Security Company #3

(U) VOIP Company

(U) Speech Recognition Company

QUESTIONS