Are We (*Really*) At Cyber War?

Dr. Julie E. Mehan, PhD
11/12/2010

Tonight’s Questions

- "What do you believe are the essential elements of a cyber security strategy that are necessary to fight and win today's cyber war?
- Are we winning the cyber war?"

Alternative Questions

- I think the real questions might be:
  - What really is cyber war and are we in one?
  - What are the essential elements of a cyber security strategy and policy that will allow us to address all forms of cyber threats?

Converging Cyberspace

Cyberterror

Cyberwar

Cybercrime

Does Not
Stand Alone

Cyberespionage

2007 - Joint Strike Fighter Compromised

- Compromise reported April 2009, started as early as 2007

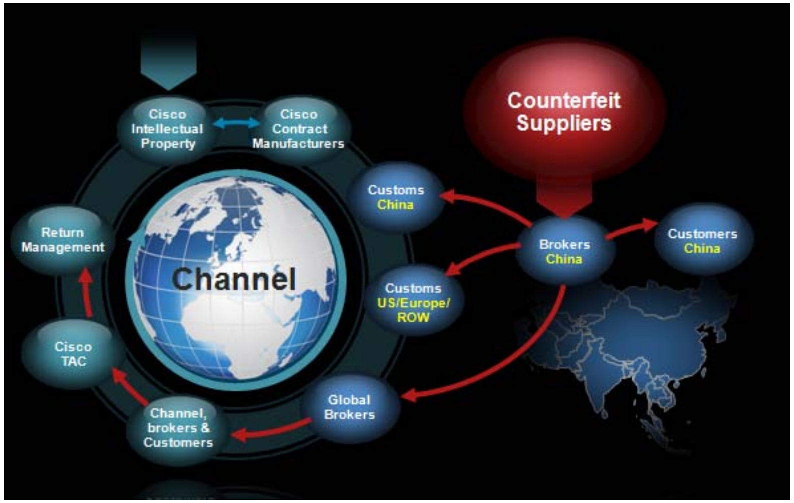
- $300 Billion project – costliest in US DOD history

“United States is under cyber-attack virtually all the time, every day”
- Robert Gates Secretary of Defense

- Several Terabytes of data stolen about electronic systems
  - Most sensitive secrets not compromised
- Source of attacks appears to be China

2008 – Operation Cisco Raider

- The Feds confiscated more than $75 million of counterfeit Cisco networking gear. The announcement is in a progress report on a two-year-old investigation, code named Operation Cisco Raider. In most cases the fake gear was made in China and imported into the United States where unethical resellers passed it off as legit.
- Intercepted the counterfeit hardware at ports of entry and dismantled illegal supply chains in the US



2008 - Crash of Spanair JK 5022

- Crash of Spanair Flight 5022 at Madrid International Airport on August 20, 2008, killing 154, found that the airline’s central computer system used to monitor technical problems in its fleet was infected with malware

Source: Defense Tech, 20 Aug 10

2008 - Thumb Drive Attack Compromises DoD Computers

- Revealed by DepSecDef William Lynn in Sep/Oct 10 Foreign Affairs Magazine
- A USB flash drive infected with Agent.btz was inserted into a U.S. military laptop at a base in the Middle East
  - "The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command."
- Spread to classified and unclassified computer systems ; ?? information exfiltrated

FOREIGN AFFAIRS

Remaking the Middle East

New Challenges Call for New Policies. Are the U.S. and Israel Ready to Change Course?

Beyond Moderates and Militants

Robert Malley & Peter Harling

How to Handle Hamas

Daniel Byman

Legitimizing Israel's Bomb

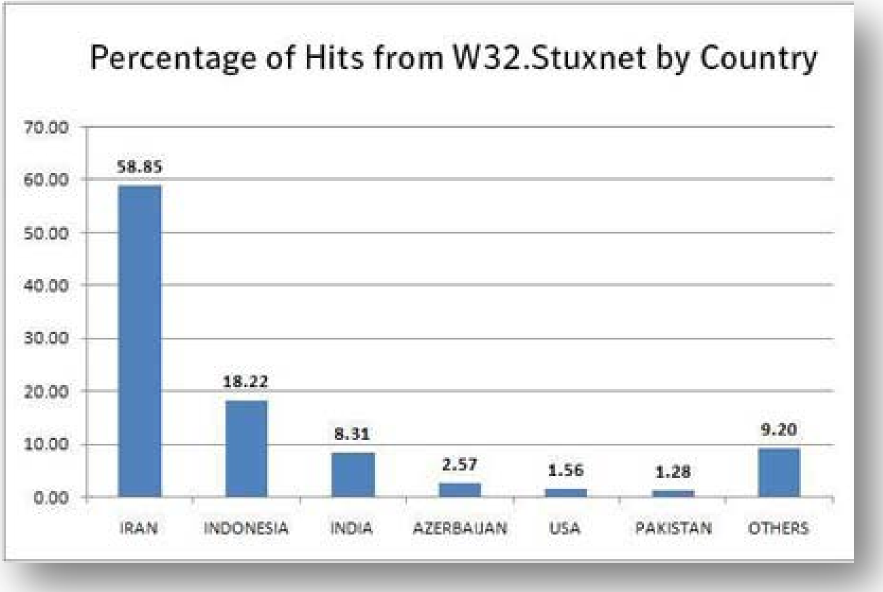
Avner Cohen & Marvin Miller

A U.S.-Iranian-Turkish Alliance?

Mustafa Akyol

2010 – Stuxnet Malware

- First malicious computer code specifically created to take over systems that control the inner workings of industrial plants
- Actively targeted Windows PCs that managed large-scale industrial-control systems in manufacturing and utility firms
- Iran appeared to be primary target
- Possibly work of state-backed professionals



A Unique Threat

- Unfettered access to cyber weapons systems (i.e., computers and Internet access)
- Immense armies (i.e., botnets that can be captured or rented)
- Capacity for attacks to strike at our nation's most strategic vulnerabilities

Challenges We Face

- IT security arms race - the bad guy is motivated… and patient
  - the adversary able to focus time and money on attacks while the target has to prioritize spending on IT security among other budget items
- Blended Cyber Threats – changing attacks
  - Technology and methods of attack always changing. Can combine several methods of attack

Reality Check

- Nature of cyberspace and cyber attacks make prediction, retaliation, deterrence and preemption difficult
  - Attacks are stealthy and unpredictable – what do you protect?
  - Source of attack difficult to pinpoint – how can a counter-attack be justified?
  - Attacks are asymmetric – who has the real risk?
  - Attacks are distributed – who can be blamed?

We Need A Cohesive Strategy

Mike McConnell, former DNI, stated:

"The United States is fighting a cyber-war today, and we are losing. It's that simple. The problem is not one of resources; even in our current fiscal straits, we can afford to upgrade our defenses. The problem is that we lack a cohesive strategy to meet this challenge."

Some Options for Action

- Deploy information systems developed to not just be functional but secure
  - Bolting on security or patching vulnerabilities is just the digital equivalent of the Maginot line
- Establish a more secure and resilient digital infrastructure
- Protect the information – not only the shell that houses it
- Insist on a secure supply chain
- Improve application level security and software assurance
- Make security transparent as possible – if security is inefficient, inconvenient, and inflexible in time of crisis if will guarantee that users will seek ways around the rules

A Necessary Paradigm Change

- Stop being defeatist.
  - Don't accept a state of insecurity and technological inadequacy.
- Work an attitude change in the private sector.
  - Government must partner with the private sector and hold the critical private sector systems accountable.
- Change the attitude of the general public.
  - Create an understanding that there may need to be an exchange of convenience for security.

References

- Claburn, Thomas. Operation Cisco Raider Nets $76M in Fake Gear. Information Week, February 2008
- Fallier, Nicolas; O Murchu, Liam; and Chien, Eric. W32 Stuxnet Dossier. Symantec, November 2010
- Gorman, Siobhan; Cole, August; and Dreazen, Yochi. Computer Spies Breach Fighter Jet Project. The Wall Street Journal, April 2009
- Habinger, Eugene. Cyberwarfare And Cyberterrorism: The Need For A New U.S. Strategic Approach. CSI, February 2010
- Lynn, William. Defending a New Domain. Foreign Affairs, September/October 2010
- McConnell, Mike. How to Win the Cyberwar We're Losing. The Washington Post, February 2010
- Meyer, David. Report: Trojan a factor in fatal Spanair crash? Cnet News, August 2010
- War in the Fifth Domain. The Economist, July 2010