Cyberthreats: The New Strategic Battleground

Lawrence A. Husick, Esq.
Co-Chair, FPRI Center on Terrorism
May 1, 2015

We were warned…

"Electronic Pearl Harbor…is not going to be against Navy ships sitting in a Navy shipyard.

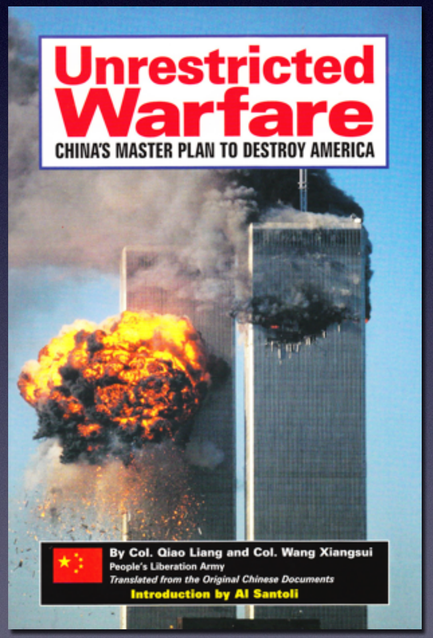
It is going to be against commercial infrastructure."

Dep. Defense Secretary John Hamre, 1999

Unrestricted Warfare

Cols. Qiao Liang and Wang Xiangsui,
People's Liberation Army of China, 1999

- Computer virus, worm, trojan
- Information poisoning
- Financial manipulation
- Direct cyberattack on US
- Based on US Strategic Concept of MOOTW (Military Operations Other Than War)



FPRI

CyberWar

"There's no agreed-on definition of what constitutes a cyberattack. It's really a range of things that can happen, from exploitation and exfiltration of data to degradation of networks, to destruction of networks or even physical equipment…"

- Dep. Defense Sec. Wm. J. Lynn, III, Oct. 14, 2010

Cyberdefense

"There is virtually no effective deterrence in cyber warfare, since even identifying the attacker is extremely difficult and, adhering to international law, probably nearly impossible.

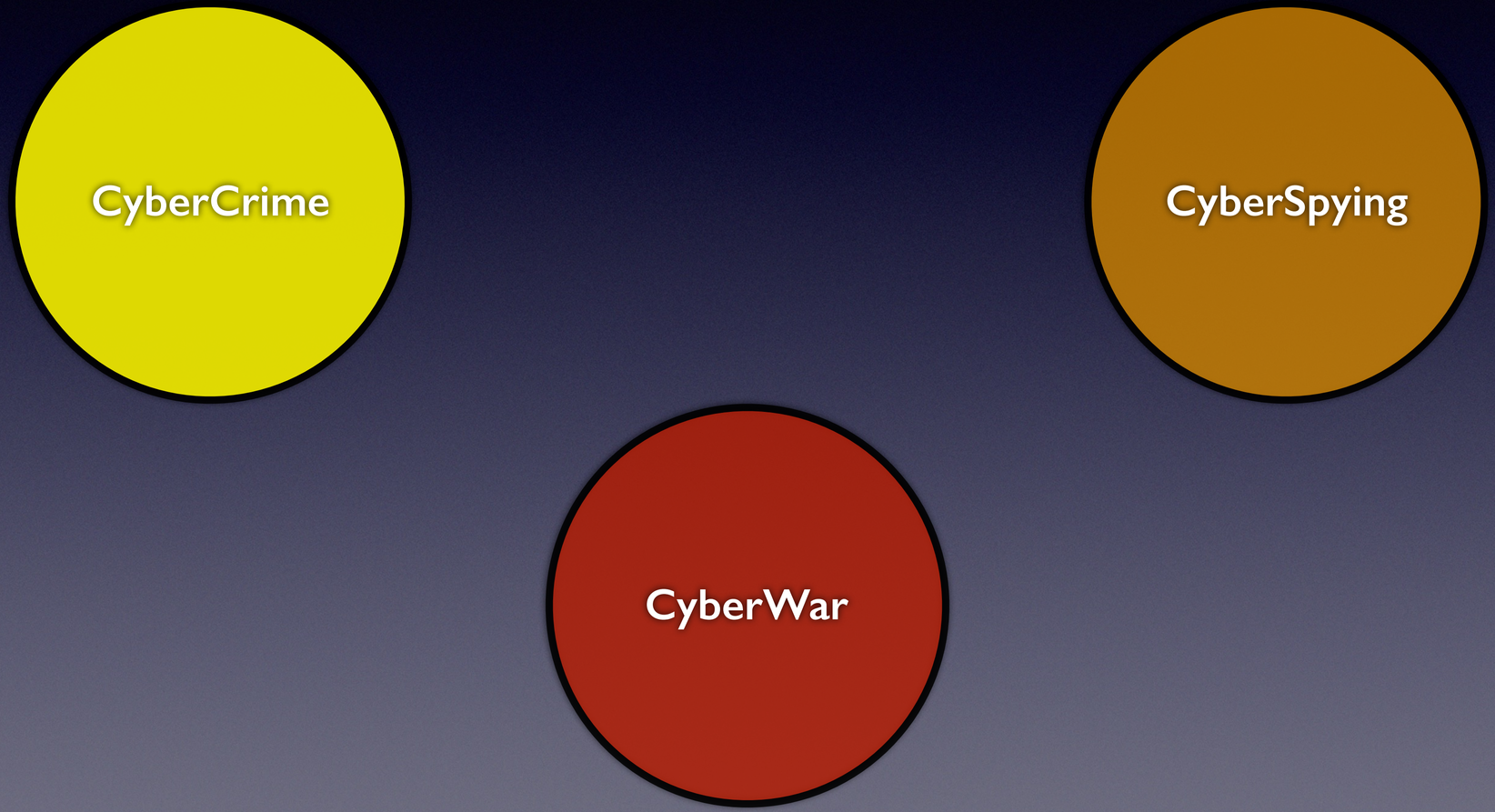
- Dr. Olaf Theiler, NATO Operations

China

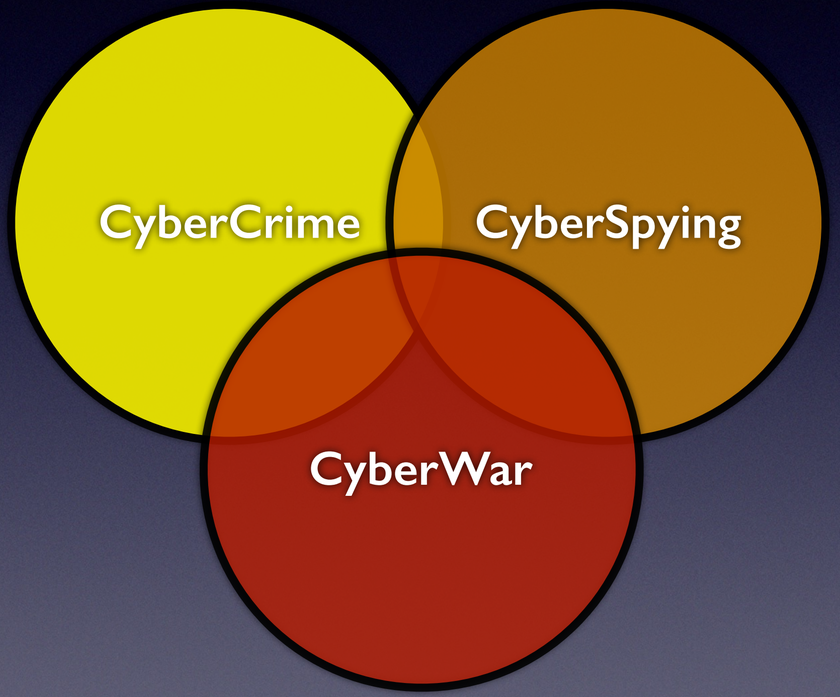
- PLA Unit 61398, located in Shanghai's Pudong area
  - Attacked over 1,000 servers using 849 addresses
  - One victim was accessed for 4 years, 10 months
  - Largest single data theft: 6.5TB

"The [Mandiant] report, … lacks technical proof. … Second, there is still no internationally clear, unified definition of what consists of a 'hacking attack'. There is no legal evidence behind the report subjectively inducing that the everyday gathering of online (information) is online spying."

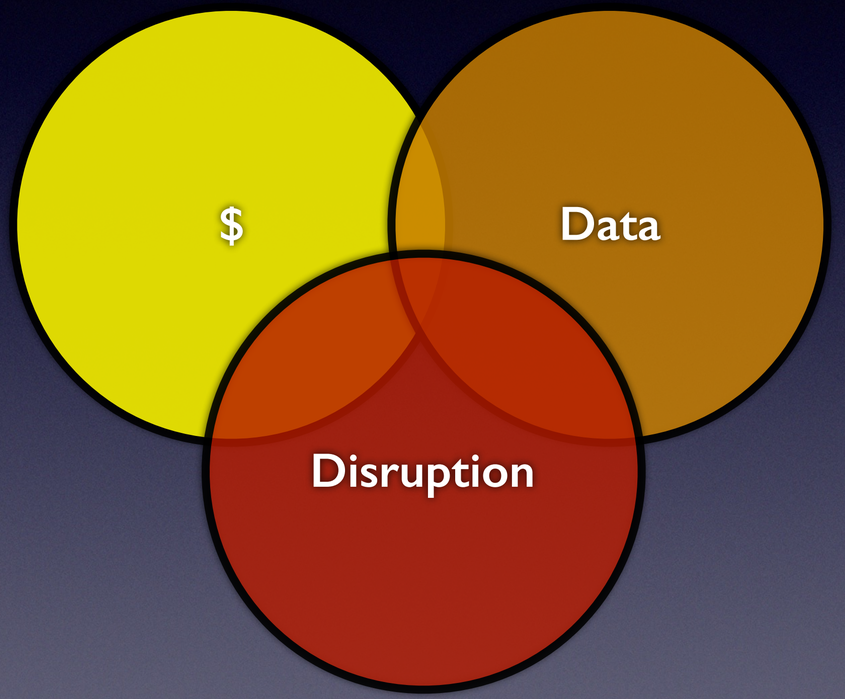
CyberThreat



CyberThreat



CyberThreat



Also:

- CyberEspionage
- CyberTerrorism
- CyberActivism
- CyberAnarchy

MAD to MUD

(Gale & Husick, Feb. 2003)

Cold War:

Mutually **A**ssured **D**estruction

Deterrence Response Model

vs.

Post Cold War:

Multilateral **U**nconstrained **D**isruption

No Clear Response Model

"There is no MAD in the Cold War sense. You can't be 'assured' of attribution. The attack can be anonymous. It can be spoofed."
– Scott Borg, CEO US Cyberconsequences Unit

Supervisory Control and Data Acquisition

"The threat to our SCADA infrastructure is demonstrable. We must act to improve SCADA security in effective and efficient ways."

- *Gale and Husick, 2003 FPRI Report*

Control systems are a particular worry, because these are the computer systems that manage physical processes. Shutting these systems down is a nuisance. Causing them to do the wrong thing at the wrong time is much worse.

- Scott Borg, Chair-US CyberConsquences Unit, DHS

“Stuxnet”

Stuxnet

Project codename: Olympic Games

Co-developed by NSA and IDF Unit 8200

Stuxnet

Operational Timing

Every ~15 minutes, Stuxnet tries to find the right PLC type, and if found, modifies the code and data on the PLC

The modified PLC then watches for the centrifuges run between ~810Hz and ~1210Hz

It then waits about 13 days before it sets the speed to 1410Hz, then 2Hz, then 1064Hz, and repeats this sequence

Stuxnet then waits 26 days before running the cycle again

Stuxnet

Consequences

P-1 centrifuge:
1410 Hz = rotor failure

Change from 1410 to 2Hz
Centrifuge contents are evacuated
Vibrations damage bearings

Iran built more than 10,000 centrifuges but fewer than 3,700 were reported to be operational in late 2010 - design since changed

Blowback: Shamoon

Initiated August 16, 2012 at Saudi Aramco
(Laylat al-Qadr, Night of Power at the end of Ramadan)

Attacks Windows NT, XP, Vista, 7

Introduced by privileged insider

Exfiltrates specific file data, erases files

Overwrites master boot record to kill computer

Destroyed 30,000 computers at Saudi Aramco,
and later, others at RasGas (Qatar)

FPRI

Blowback: Other Attacks

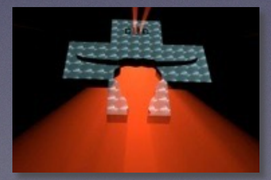
Qassam Cyber Fighters - DDoS attacks against BB&T, Capital One, Ally Financial, Bank of America, JPMorgan, SunTrust, PNC, RegionsBank

Syrian Electronic Army - DDoS attacks against BBC News, the Associated Press, National Public Radio, Al Jazeera, Financial Times, The Daily Telegraph, The Washington Post, Syrian satellite broadcaster Orient TV, and Dubai-based al-Arabia TV, Human Rights Watch

FPRI

Hacktivism

Anonymous, LulzSec, Legions of the Underground, Cult of the Dead Cow, L0pht Heavy Industries, Chaos Computer Club, AntiSec, others…



Where Are We Now?

95%+ of systems are non-government

Most PCs run Windows, and cannot be effectively secured - 40% run pirated copies

Windows XP support ended in April 8, 2014, yet 20% of users still operate that version

XP and Office 2003 no longer receive security updates

Windows 7 no longer supported

There are now over 75 million unique malware files

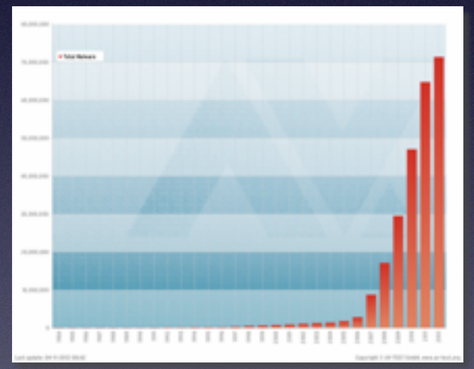
17% of all legitimate PCs run no protection at all!

FPRI

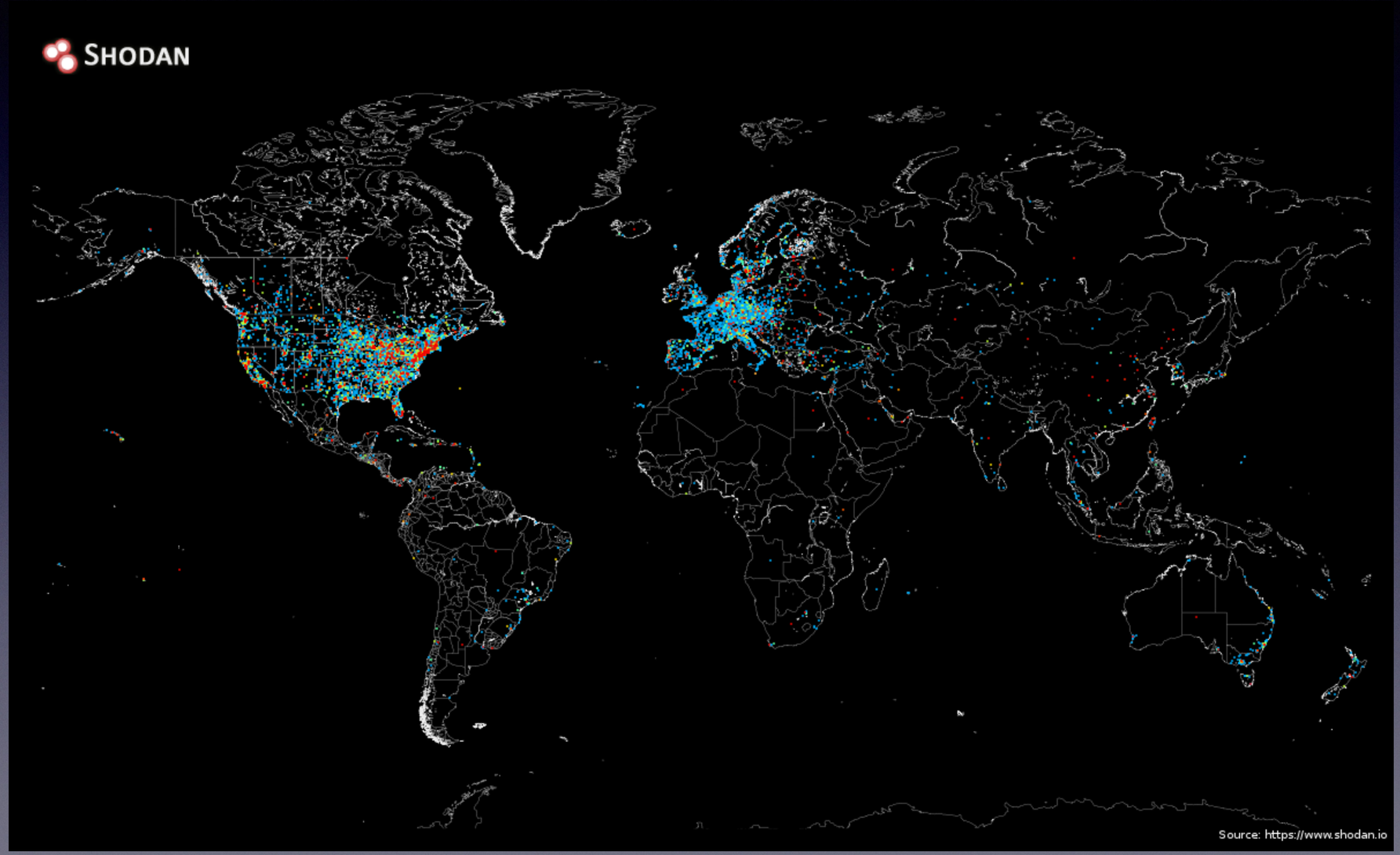
Where Are We Now?

More “malware” was released in 2014 than in all prior years combined.

SCADA networks and industrial controllers are difficult and costly to secure, many must be replaced entirely to achieve security, hardware may be compromised - thousands of SCADA systems are on the Internet!



SCADA On the Internet



Off-Shore Oil Rigs Have Been "Incapacitated" By Malware Thanks To Pirated Music and Porn

"They literally had a worm that was flooding their network, and they're out in the middle of the ocean."

Is it War?

"*If you shut down our power grid, maybe we will put a missile down one of your smokestacks*," an unnamed military official told the Wall Street Journal.

"LOLZ…we haz 0 smokestacks, dude!"

- an unnamed hacker, in response

US Cyberstrategy

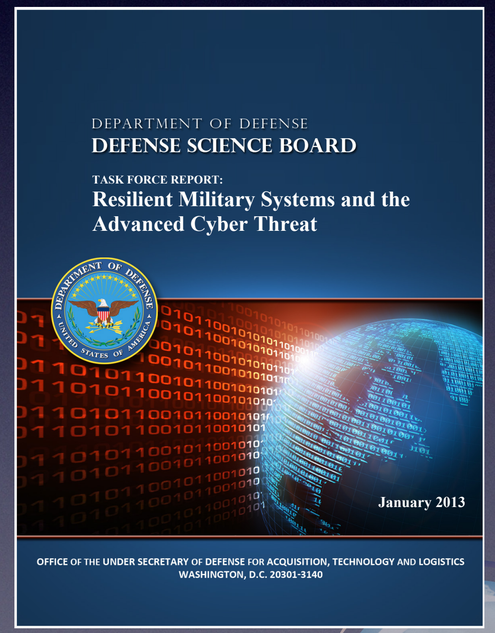
"As a matter of principle, the United States will seek to exhaust all network defense and law enforcement options to mitigate any potential cyberrisk to the U.S. homeland or U.S. interests before conducting a cyberspace operation, but there may be times when the president or the secretary of defense may determine that it would be appropriate for the U.S. military to conduct cyberoperations to disrupt an adversary's military related networks or infrastructure so that the U.S. military can protect U.S. interests in an area of operations. For example, the United States military might use cyberoperations to terminate an ongoing conflict on U.S. terms, or to disrupt an adversary's military systems to prevent the use of force against U.S. interests."


WE'RE WORKING ON MILITARY RESPONSE!
HACKERS
Google
PENTAGON CYBER STRATEGY
PARESH

How Vulnerable?

"Our nuclear deterrent is regularly evaluated for reliability and readiness. However most of the systems have not been assessed against a Tier V-VI cyber attack to understand possible weak spots."

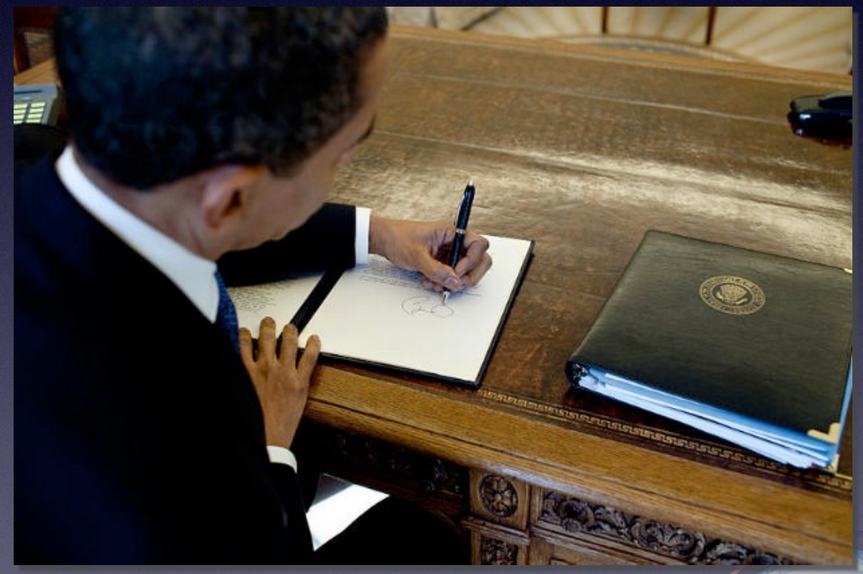
- Defense Science Board, Jan. 2013



FPRI

Cybersecurity Executive Orders

- Follows twice-filibustered bipartisan cybersecurity legislation in 2012
- Mostly aspirational
- NIST to create "frameworks" for voluntary use by private sector
- Freeze assets if you can figure out who the bad guys are



Crystal Ball Gazing…

Nearly all future wars will see the use of cyberweaponry as a disrupter or force multiplier.

Preventative and detective security technologies will not provide protection against all the threats; considerable effort will be needed to mitigate and recover from losses

Most of the time it will be impossible to ascertain the identity of the attacker. This means that a defense doctrine based on deterrence will not work

- Sommer & Brown, Reducing Systemic Cybersecurity Risk, OECD Report 14-Jan-2011

Conclusions

Cyberthreats are just threats that use computers and networks as a tactic. It's easy to do!

The are only minor differences among cybercrime, cyberespionage, cyberterrorism, and cyberwar.

Cyberthreats are asymmetric - the West is highly computerized and networked, much of the rest of the world is not. Non-state actors are mostly immune.

Retaliation is usually not possible.

The Private Sector is playing catch-up, badly.

We've been warned…

"Our country will…at some point, face a major cyber event that will have a serious effect on our lives, our economy, and the everyday functioning of our society."

Outgoing DHS Sec. Janet Napolitano,
Aug. 27, 2013


FPRI


FPRI

Questions?

lhusick@fpri.org