Cyber-crime, Cyber Terrorism, and Electronic Espionage: Has a Cyber War Already Happened?

David Willson
Attorney at Law
CISSP, Security +
Titan Info Security Group
Who Am I?
This briefing is not an answer to ALL questions, but instead poses some issues to think about and hopefully puts the issues in a more clear perspective.

Most of the issues discussed continue to be discussed in international circles as no one has been able to come to a clear and concise solution or conclusion.
So, where do we draw the line?

When does a cyber attack cross the line from hacking, cyber crime, or electronic espionage and become an **ACT of WAR??**
A Crippling Cyber Attack Would Be an 'Act of War' - Leon Panetta

See video here:

Leon Panetta Cyber War Question
Defining Cyber War

DoD: Cyberattack on U.S. could warrant deadly response
(Unidentified military officials speaking with The Wall Street Journal)

“If you shut down our power grid, maybe we will put a missile down one of your smokestacks, . . . .”

(Chris Carroll, Stars and Stripes, May 2011)
Headlines!

- Georgia
- Estonia
- Shamoon
- North Korea
- STUXNET /OLYMPIC GOLD
- Google
- RSA
- Flame
Headlines!

- WannaCry
- Panama Papers
- Petya
- OPM
- Vault 7 (CIA Doc Dump)
- Yahoo
- DNC
- Dyn
Digital Spies: The Alarming Rise of Electronic Espionage

“Foreign agents are stealing stealth technology, hacking heads of state, and sabotaging American companies. And while many of these attacks are traced to China, electronic espionage is an accelerating scourge that knows no national boundaries.”

(Adam Piore, Popular Science, Jan. 24, 2012)
Recent Headlines!!

Operation Shady RAT
(By Dmitri Alperovitch, Vice President, Threat Research, McAfee)

An investigation of targeted intrusions into more than 70 global companies, governments, and non-profit organizations during the last five years
U.S.

Cyber-spying by China and Russia a threat

“Billions of dollars of trade secrets, technology and intellectual property are being siphoned each year from the computer systems of U.S. government agencies, corporations and research institutions to benefit the economies of China and other countries,” the Office of the National Counterintelligence Executive said.

(By Ellen Nakashima, Washington Post, Nov. 4, 2011)
Hack at Illinois Water Plant Shows Vulnerabilities in Critical Infrastructure

Allegedly, hackers based in Russia were able to remotely shut down a water pump at a facility near Springfield.

(Sue Marquettte Poremba Nov 21, 2011 - Reuters)
Recent Headlines!! - Shamoon

(Reuters 7 Sept 2012) - One or more insiders with high-level access are suspected of assisting the hackers who damaged some 30,000 computers at Saudi Arabia's national oil company last month, sources familiar with the company's investigation say.
Recent Headlines: Call for Cyber

“Army and Marines creating systems for cyber fire support”

(Foreign Policy: Posted By John Reed Monday, September 10, 2012)
Recent Warnings!!

Utilities

Oil Companies

National Infrastructure

F35 Joint Strike Fighter
Cyber Pearl Harbor?

Eric Rosenbach, Deputy Assistant Secretary of Defense for Cyber Policy:

“A catastrophic cyberwar is important to prepare for, but an unlikely scenario. Stealing data important to the nation’s economic security, meanwhile, is occurring here and now!”

(National Defense July 2012)
**UN Charter**

**Art. 51 Self-Defense**

**Geneva Convention**

**Customary Int’l Law**

**LAW**

**Hague Convention**

**Anticipatory Self-Defense**

See: Talinin Manual
Use of Force v. Armed Attack

1. **Use of Force**: in response a nation may use lesser or equal means as compared to the original use of force (probably would not allow a kinetic response to a cyber attack considered a “use of force”)

2. **Armed Attack**: allows the attacked nation to respond with a proportional response (if cyber attack is considered an “armed attack,” the attacked nation can likely respond with a kinetic attack)
Use of Force v. Armed Attack

Issue: When does a cyber-attack equal an “armed attack?”

Theory: Any cyber-attack that may have the same result as a kinetic attack would likely be classified as an “armed attack”
Is this electronic espionage or an act of war?

- Defacing your adversary’s website? (Happened)
  - Use of Force – Armed Attack?

- Blocking their Internet access to the outside world? (Happened)
  - Use of Force – Armed Attack?

- Stealing their military secrets? (Happened)
  - Use of Force – Armed Attack?
Is this electronic espionage or an act of war?

• Planting logic bombs in critical infrastructure?
  (Happened? Some say yes)
• Use of Force – Armed Attack?

• What about in defense hardware and software: communication satellites, missile defense, etc.
• (Has it happened??? Some say yes!!)
• Use of Force – Armed Attack?
Is this electronic espionage or an act of war?

Disrupting an adversary’s financial structure?
  Use of Force – Armed Attack?

Erasing an adversary’s critical data?
  Use of Force – Armed Attack?

What about disrupting or even altering GPS?
  Use of Force – Armed Attack?

How about “challenging our ability to operate freely in the cyber commons?”
  Use of Force – Armed Attack?
Is this electronic espionage or an act of war?

How about disrupting or setting back your adversaries nuclear weapons program, or what they say is just nuclear power??
Dubai: The US will face a “teeth-breaking” response if it continues to carry out cyber attacks against Iran, an Iranian official said Wed.

“If the Americans’ futile cyber attacks don’t stop, it will face a teeth-breaking response,” . . . . (Iranian Students News Agency)
Do We Have a War?

If a tree falls in the woods and no is there does it make a sound?

If one nation attacks and the other does not respond do we have a war?
Critical Piece
Do you know who is attacking you?
Attribution (can you fire back blindly?)

“Sum of All Fears”  (See movie trailer here:
http://www.youtube.com/watch?v=8GPu-oZ4p64

In this movie, terrorists made it appear that Russia detonated a nuclear weapon in Baltimore. This deception almost led to the US and Russia launching nuclear attacks on one another. Deception in cyberspace is much easier.
Is this electronic espionage or an act of war?

How about selling electronics with a surreptitious back door??
How about selling drones that automatically upload camera feeds to a website that the nation-state accesses and copies? Is this electronic espionage or an act of war?
What About Precedence?

In the 90’s a Russian professor declared that Russia considers information operations (the term used at the time) to be akin to a nuclear attack and retains the right to respond with a nuclear strike.
Recap

1. Has a cyber war already occurred?

2. Can we draw a clear line?

3. What factors must inevitably be considered?
   a. Attribution
   b. Escalation
   c. Setting precedence
Recap

Stuxnet/Code
Yellow/Shamoon

Act of War/
Use of Force/
Armed Attack??
Use of Force v. Armed Attack

Use of Force: I would argue that most of what we see in the news that is labeled a “cyber-attack” or “cyber war” could be considered a “use of force,” thus allowing the aggrieved nation to respond in kind.

Question: is the use of Stuxnet then considered a “use of force?” Yes

How about an “Armed Attack?” This question is yet to be answered!!
What will it Take?

No single incident

Combination of attacks

Rise to level of do or die or economic Armageddon!
Assuming we are not at war, then this is a Risk Management problem for companies.

How do you manage this risk?

Develop and implement ROE for your company. E.g. have a plan!
• Businesses are on their own

• Govt has its hands full

• What can companies do?

• Active Defense!!
  (Take the fight to the bad guys)
David Willson
Attorney at Law
CISSP, Security +
Titan Info Security Group
719-648-4176
david@titaninfosecuritygroup.com
www.titaninfosecuritygroup.com
Or TEXT the Words
“Titansecurity” to 50500

Property of Titan Info Security Group