SECURE360 conference

RON WOERNER
CYBER WAR! YES, IT'S HAPPENING NOW!
WEDNESDAY, MAY 14, 1:30 PM, ROOM 14

Like what you hear? Tweet it using: #Sec360
These are my thoughts…
NOT A DEBATE ABOUT NSA & SNOWDEN
This is based on open-source materials…
This Briefing is:

UNCLASSIFIED
MILKEN 2014: RUSSIA COULD WAGE CYBER WAR ON U.S.

LOS ANGELES -- Russia, enraged by the Obama administration's sanctions over Ukraine, could strike back at the U.S. via cyber warfare -- then deny the attack ever took place, a former top intelligence official said Tuesday.

Russia, considered the second country most adept at cyber warfare after the U.S., could use an attack on American computer systems as a way to seek revenge on the U.S., said Richard Clarke, a top counter-terrorism and intelligence official for both the Clinton and George W. Bush administrations.

Former Defense Secretary Leon Panetta, who joined Clarke and former National Security Agency Deputy Director Chris Inglis at the Milken Institute Global Conference here, says Russia is no different than the U.S. when it come to its attitude toward cyber warfare. It's a key element of its strategy.

The Russians already used it during in dealing with Georgia and Crimea, Panetta said. If Russia decides on military action against Ukraine, “cyber would be part of that.”

Treat cyberspace like a battlefield

CYBERSECURITY KILL CHAINS

What is:

WAR?

= or ≠

CYBERWAR?
DOD CYBERSPACE DEFINITION

A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

(Joint Publication 1-02, DoD Dictionary of Military Terms, Washington, D.C.: Joint Staff, Joint Doctrine Division, J-7, October 17, 2008.)
CYBER WARFARE DEFINITIONS

Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.
Richard A. Clarke, “Cyber War”

The art and science of fighting without fighting; of defeating an opponent without spilling their blood.
Jeffrey Carr, “Inside Cyber Warfare”
RELATED TERMS AND ISSUES

Cyber-terrorism – parallel definition, different actor
- actions by *terrorists* to penetrate another nation's computers or networks for the purposes of causing damage or disruption

Cyber-spying / cyber-espionage
- actions by *parties outside of a country or organization* to penetrate another nation's computers or networks for the purposes of stealing information
RELATED TERMS

Strategic Cyberwar
- Cyberattacks to affect state policy
- Takes place among combatants who are not fighting a real—that is, physical—war

Operational Cyberwar
- Cyberattacks to support war fighting

“Cyberdeterrence & Cyberwar,” Martin Libicki (2009), RAND
Weapons of Mass Disruption
Weapons of Mass Annoyance
ACTS OF WAR?
WEBSITE DEFACEMENT – IS IT WAR?

**Mirror saved on:** 2008/08/18 01:30

<table>
<thead>
<tr>
<th>Defacer</th>
<th>Domain</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agd_Scorp</td>
<td><a href="http://dodtravelregs.hqda.pentagon.mil/t">http://dodtravelregs.hqda.pentagon.mil/t</a></td>
<td>141.116.10.20</td>
</tr>
<tr>
<td>System: Win 2003</td>
<td>Web server: Unknown</td>
<td></td>
</tr>
</tbody>
</table>

**Attacker stats**

---

**Terrorist Crew**

---

Hacked by | Agd_Scorp, JeXToxiC, Wh0!, Starturk, Rx5, AntiW4R, Security-Terror

Gr33z to: Kerem125, Gey, Oscar Sanders, CoRR@il, The BokiB, el-CD
“BOTS” & “BOTNETS” – ARE THEY AN ACT OF WAR?
"ANONYMOUS" ATTACKS – IS IT WAR?

http://anonops.blogspot.com/
RELATIONSHIP TO TRADITIONAL WARFARE

Cyberwar an additional domain in traditional warfare.

Used as initial stage to:
- reduce command and control facilities,
- harm national infrastructure,
- spread propaganda,
- deflect real dangers,
- reduce confidence in government.
INFRASTRUCTURE SUBJECT TO ATTACK

- Military command and control system
- Transportation systems
- Power grid
- Businesses
- Manufacturing facilities
- Communication systems
- ...

RON WOERNER – CYBERWAR 2014

5/21/14
Treat cyberspace like a battlefield

CYBERSECURITY KILL CHAINS

A "KILL CHAIN" ANALYSIS OF THE 2013 TARGET DATA BREACH

THREE EXAMPLES OF POSSIBLE CYBERWAR ACTIVITY

1. Titan Rain (2003-on)
2. Estonia (2007)
1. TITAN RAIN (2003-ON)

Coordinated attacks on US military and industrial computer systems
Access gained to computer systems and networks including Lockheed Martin, Sandia National Laboratories, and NASA
Purpose and identity of attackers remains unclear, though origin appears to be Chinese military
2) ESTONIA (APRIL 2007)

Sometimes referred to as “Web War 1”
Followed Estonia relocating the Bronze Soldier of Tallinn, a Russian monument
Sophisticated and large set of denial of service (DoS) attacks on Estonian parliament, banks, ministries, newspapers, other web sites
Severe effect on above institutions for approximately three weeks
3) STUXNET WORM

Very complex Windows-specific computer worm that infects computers and connected industrial control equipment (PLCs)

Spreads through USB thumb drives as well as network connections

Utilizes four “zero-day” exploits

Uses stolen valid security certificates
3) STUXNET WORM (CONT.)

Initial high rate of infection in Iran, specifically found at nuclear facilities
- May be government (Israel, US, UK?) attempt to damage Iranian nuclear facilities
- Unclear if delay or damage actually occurred

Worm has spread to many other countries (including large infection of Chinese systems)
POLITICAL ISSUES

Is the threat of cyberwar overstated?

Marc Rotenberg (Electronic Privacy Information Center)

Bruce Schneier (Chief Technology Officer, BT Counterpane)
Much hyperbole, “sexy” news

Little distinction between cyberwarfare, cyberspying, cybercrime, and hacking

Threats today are more from cyber-espionage & cybercrime

Used to generate additional funding for U.S. cyberdefense efforts

Used to justify efforts to give U.S. government more control over Internet
DIFFICULTIES IN DEFENSE

• Large Threat Landscape
• Difficult to trace attacks
  ▪ Many from botnets on compromised PCs
• Internet created for convenience, not security
  ▪ Internet technology does not support easy defense
• Unknown capabilities of other nations & groups
  ▪ Role of Cyber Deterrence
Difficulties in Defense for USA

Internet created in USA in an environment of intellectual freedom, mostly under private (not government) control

- Efforts to change
  - “Kill Switch” bill (2010)
- Other countries can more easily mount defense
  - Great firewall of China
DISINCENTIVES TO CYBERWAR

Deterrence & Mutually Assured Destruction
- Potential for retribution

Harming the Internet tends to harm everyone
- Difficult to contain scope of cyberattacks
- Collateral damage

Non-cyber interests are connected
- China owns significant portion of U.S. financial structure
MODERATING EFFECTS ON CYBERWAR

Diversity of systems and networks
- Many networks, multiple operating systems

Increasing efforts on intrusion detection and prevention
- Early detection may help reduce scope of effects, though malware can spread quickly
WHAT

"Cyberdeterrence & Cyberwar," Martin Libicki (2009), RAND
“Cyberdeterrence & Cyberwar,” Martin Libicki (2009), RAND, p. 186
WHAT TO DO?

1. Enact limited government regulation of Internet / Cyberspace
   - Need international cooperation as well as national efforts
2. Investigate cyber-treaties
3. Increase resources for cyber-defense (government & private)
4. Isolate critical infrastructure (e.g. power grid)
REFERENCES / MORE INFORMATION


“Inside Cyber Warfare,” Jeffrey Carr (2012)

“Cyberdeterrence & Cyberwar,” Martin Libicki (2009), RAND,
NPR Morning Edition Two-Part Series

“The Online Threat”, article by Seymour Hersch

Wikipedia – Cyberwarfare & Cyberterrorism

IT Harvest – Cyber Defense Weekly
- http://it-harvest.com/CDW
Ron Woerner

- Director of CyberSecurity Studies
- Bellevue University
- ronald. woerner @bellevue.edu
- Twitter: @ronw 123

- http://academic2.bellevue.edu/~rwoerner/