CYBERTERRORISM

21 November 2012

Cyberwarfare

By Thomas Slezak

What Is Cyberwarfare?

Cyberwarfare is Internet-based conflict involving politically motivated attacks on information and information systems.

"Any country can wage cyberwar on any other country, irrespective of resources, because most military forces are network-centric and connected to the Internet, which is not secure."

- Jeffrey Carr

Types of Attacks

Sabotage - Normal operation of military and financial computer systems is disrupted. These include things such as communications, fuel, power, and transportation infrastructures.

Espionage - The use of an exploit to obtain sensitive information. This includes things like classified information.

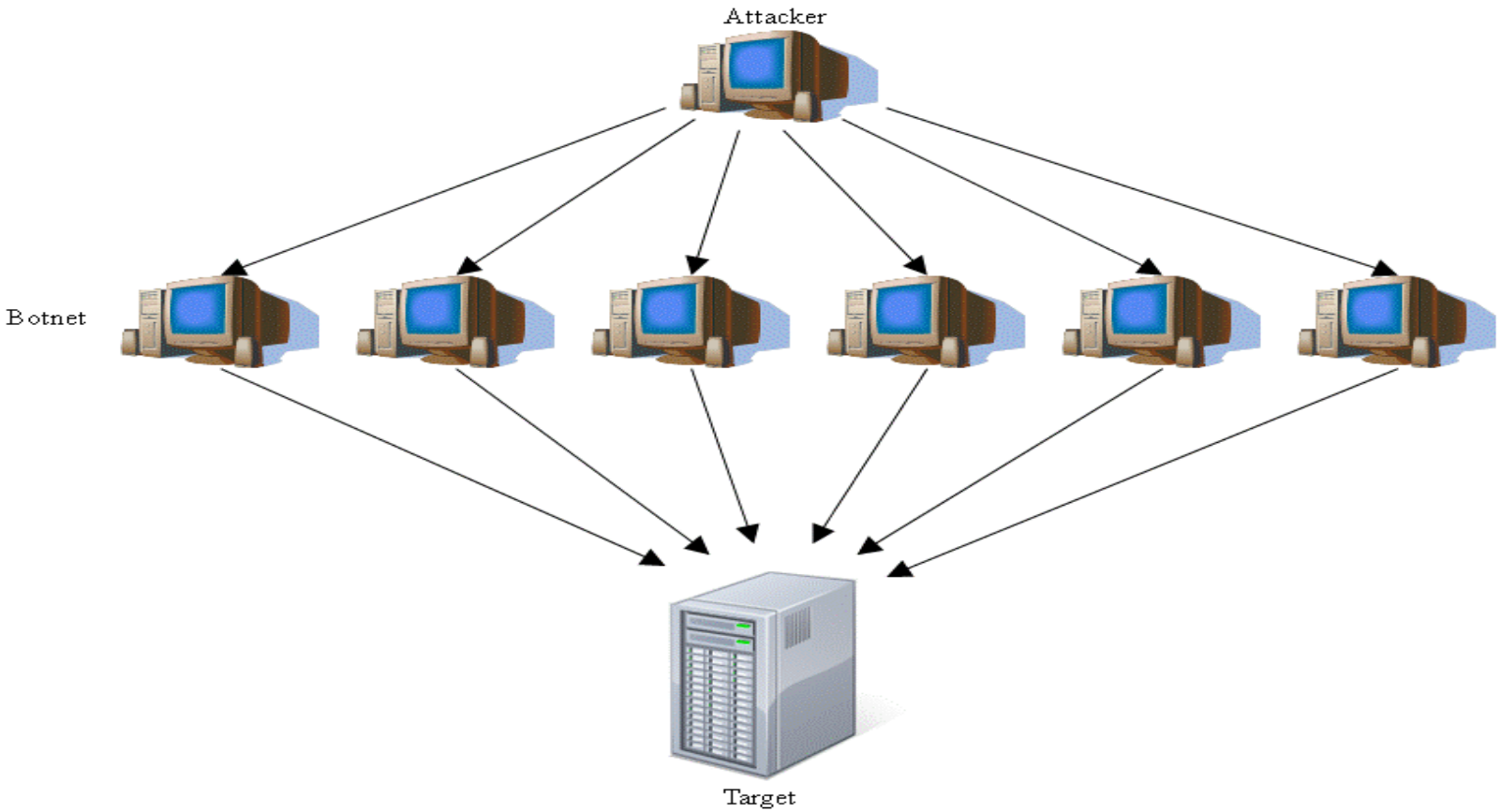
Methods of Attacks

Malware - Refers to hostile or intrusive software which can be used to spy on a system.

Denial of Service - A single computer is used to repeatedly send messages to a target, this will use up the bandwidth of the target and disrupt normal usage.

Directed Denial of Service

Figure 1 DDoS attack



Attacker sends command to botnet, botnet floods server with messages

Defense Against Cyberwarfare

Active Defenses - Take action to stop or retaliate when a system is attacked. An example of this is a honeypot, which is using a fake network.

Passive Defenses - Attempt to stop attacks from happening in the first place. Firewalls, antivirus software, and access controls are considered passive defenses.

Examples of Cyberwar Events

1973 - Defense Advanced Research Projects Agency (DARPA) starts a research program to investigate technologies for linking computer networks.

1997 - US held a cyberwar game called "Eligible Receiver."

1998 - The United States hacked into Serbia's air defense system. The US compromised air traffic control to help with the bombing of Serbian targets.

Examples Continued

2007 - Estonia was attacked by a botnet of over a million computers. Government, business, and media websites were taken down by the attack.

2009 - GhostNet, a cyber network that accessed information belonging to governments and private organizations.

2010 - Stuxnet, a new type of malicious software is identified.

References

1.http://searchsecurity.techtarget.com/definition/cyberwarfare

2.http://www.cse.wustl.edu/~jain/cse571-11/ftp/cyberwar/index.html

3.http://www.csmonitor.com/USA/2011/0307/Cyberwar-timeline

4.http://gcn.com/articles/2012/04/12/estonian-president-cyberwar-target-intellectual-property.aspx

5.http://en.wikipedia.org/wiki/Cyberwarfare

6.http://www.techopedia.com/definition/13600/cyberwarfare

STUXNET

Chris Shiplet

History

First identified by the security company VirusBlokAda in June 2010.

Brian Krebs's July 2010 blog posting was the first widely read report.

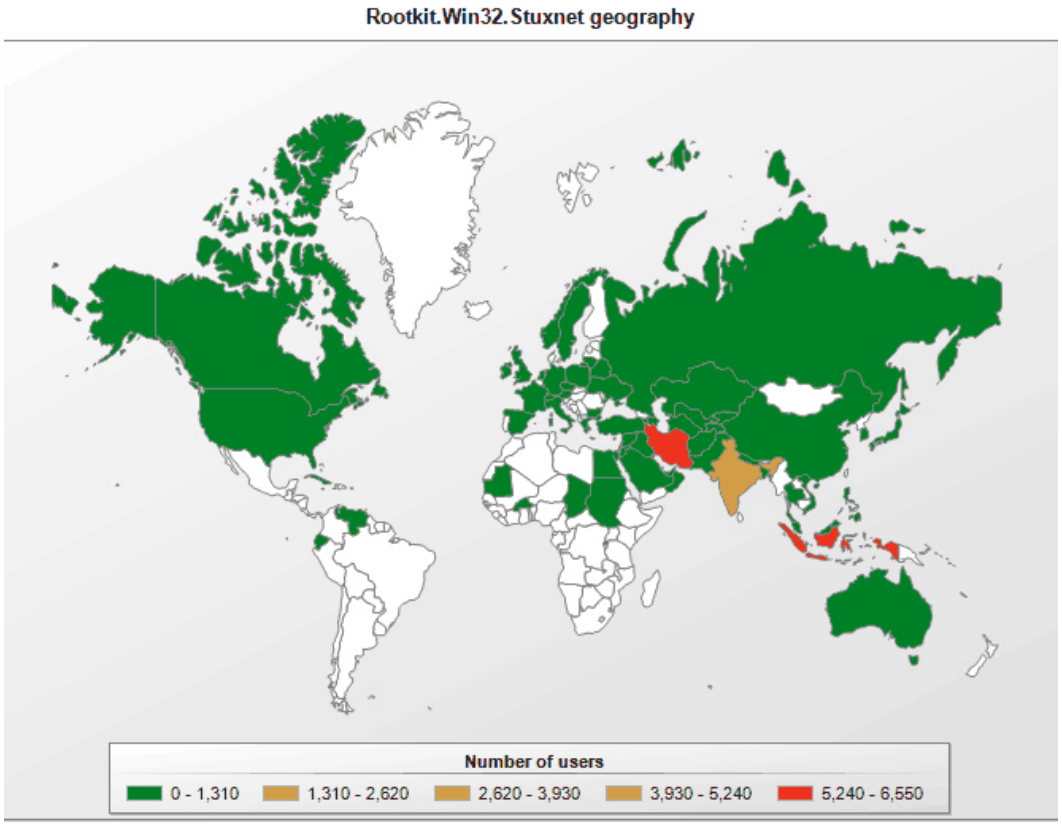
A DDoS attack from an unkown party was carried out on two leading industrial infosec mailservs the day Kreb's report was published.

Name is derived from keywords found in the software.

Symantec estimates that the group developing Stuxnet would have consisted of anywhere from five to thirty people, and would have taken six months to prepare.

First variant spread June 2009, improved version March 2010, final version April 2010.

Location



Virus Spread:

Iran 58.85%
Indonesia 18.22%
India 8.31%
Azerbaijan 2.57%
United States 1.56%
Pakistan 1.28%
Others 9.2%

Siemens PLCs

Popular Programmable Logic Controller

Universal Automation

Can be programmed via Windows software "Step7"

Used to control and monitor a wide variety of industrial devices

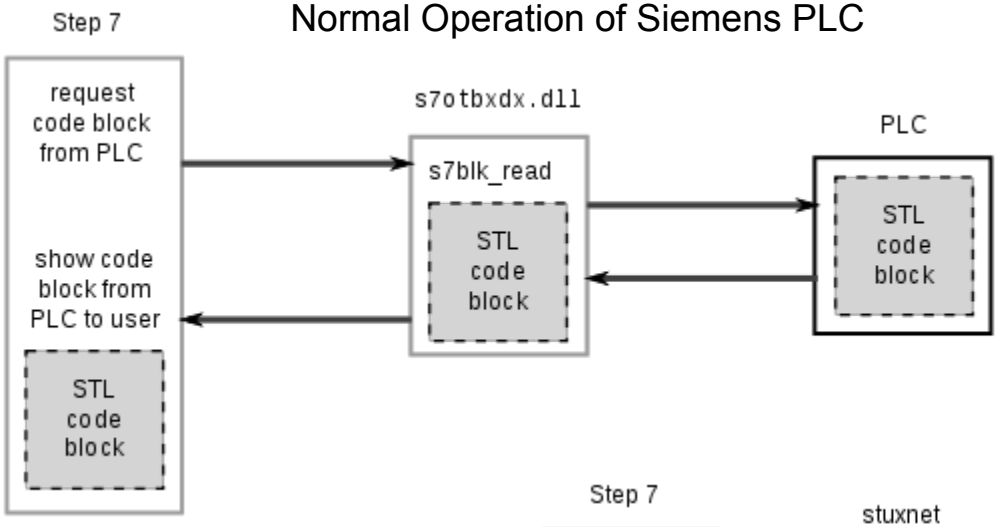
Virus Operations

- Targets PCS 7, WinCC and STEP7 software on Windows, and Siemens S7 PLC
- "Man in the middle" between Step7 and PLC
- Only attacks those PLC systems with variable-frequency drives from two specific vendors, and only those drives which run at 807-1210Hz
- Uses a zero-day exploit to install a rootkit on the PLC which hides the virus while periodically modifying the drives to run at 1410 Hz then 2 Hz then 1064 Hz, while reporting normal operation to the controller.

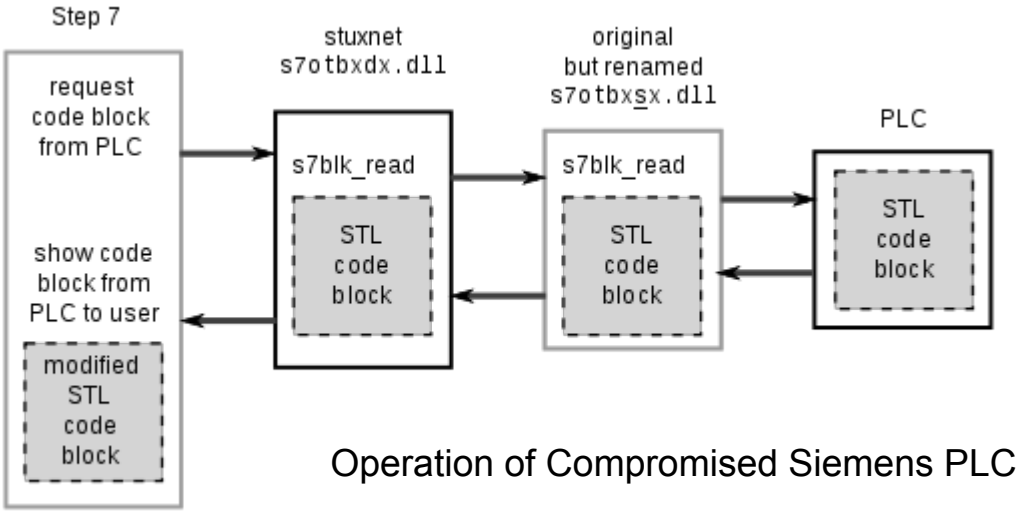
Virus Operations

- Uses four zero-day attacks to infect thumb drives and spreads to local Windows computers via P2P protocols such as RPC
- Both user-mode and kernel-mode rootkit capability
- Signed drivers with two stolen private keys from JMicron and Realtek (both located in same office park in Taiwan)
- Websites in Malaysia and Denmark used as command/control, data logging
- Becomes inert if Siemens software not installed
- Safeguards: Only spreads to 3 other computers, deletes itself in June 2012

Virus Operations



Normal Operation of Siemens PLC



Operation of Compromised Siemens PLC

Speculated Origin: US/Israeli Involvement against Iranian nuclear facility (What, Where, When... Why? How?)

- Natanz refining facility - air-gapped from outside networks
- Personal devices carried in & connected to local network... "Beacon" code mapped out Natanz and its industrial controllers
- Discovered that centrifuges controlled by S7 PLCs could be physically damaged with certain parameters
- Transferred by thumb drives
- A programming error introduced in an update led to the worm spreading to an engineer's computer that had been hooked up to the centrifuges, and then spread when the engineer returned home and hooked his computer up to the internet.

Speculated Origin: US/Israeli Involvement against Iranian nuclear facility (What, Where, When... Why? How?)

- Operatives transferred the virus to workers in the factory, who over time used their personal devices on the refinery's network, spreading the virus to Natanz systems
- US/Israel were trying to set back the Iranian research program, and the US was trying to keep Israel from launching a pre-emptive military attack.
- Number of operational centrifuges in Iran declined from about 4700 to 3900. ISIS report says Stuxnet is a reasonable explanation and may have destroyed up to 1000 (10%) centrifuges between November 2009 and January 2010.

Deaths Following StuxNet Incident

January 2010 - An Iranian nuclear scientist and physics professor at Tehran Universit killed in a bomb explosion.

November 2010 - Two Iranian nuclear scientists targeted in simultaneous car bomb attacks near Shahid Beheshti University in Tehran.

Majid Shahriari, a quantum physicist was killed.

Fereydoon Abbasi, a high-ranking official at the Ministry of Defense was seriously wounded.

January 2012 - Director of the Natanz nuclear enrichment facility, Mostafa Ahmadi Roshan, was killed in an attack quite similar to the one that killed Shahriari.

Iranian President tours Natanz

Effects

“Stuxnet was effective, but it wasn't a knockout blow... What it has done, however, is open a new front”

- Ilan Berman

"All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law."

- US Report

- Cyberwarfare that affects physical targets
- Legitimizing US cyber attacks while US criticizes others
- Source code ushered new-gen attack tools

References

Siemens http://www.automation.siemens.com/mcms/simatic-controller-software/en/step7/pages/default.aspx

Operation http://en.wikipedia.org/wiki/Stuxnet

Origins http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/

Photo http://www.nukesofhazardblog.com/story/2010/2/12/114221/466

Diagrams http://en.wikipedia.org/wiki/File:Step7_communicating_with_plc.svg

Darpa's Plan

By: Sean Rutledge

What is it?

- A five year research program
- Goal: create suite of tools for understanding, planning, and managing cyberwarfare in real-time, large-scale, and dynamic network environments
- Explicitly not funding research and development efforts in vulnerability analysis or cyberweapon generation
- In depth details not available to the general public

Cyber Battlespace

- Developing automated analysis techniques
- Assist human operators in planning cyber operations
- Analyzing large-scale logical network topology characteristics of nodes
  - Edge count
  - Dynamic vs. Static links
  - Usage
- Coordinated views for planning, operation, situational awareness, and war gaming

Cyber Operations

- Developing high-level mission plans and automatically synthesizing a mission script that is executed
- Quantify the potential battle damage
- Runs on auto-pilot and can repeat certain
- offensive and defensive functions.

Operating Systems & Platforms

- Perform cyberwarfare functions
  - Battle damage monitoring
  - Communication relay
  - Weapon deployment
  - Adaptive defense

Why is this significant?

- Cyber offense is no longer being denied but not fully discussed
- Working on offensive capabilities can help strengthen defense.
- Pre-defined battle plans and rules of engagement would allow for faster actions to be taken
- Cyber offense has a lopsided advantage over defense
  - Security packages can involve up to 10 million lines of code
  - Malicious software on average only requires 125 lines

Ethical Issues/Concerns

- Unintended consequence
  - Disruption of civilian networks
  - Shutting down a hospital generator
- Prompt other countries to step up their own programs

References

- http://www.slate.com/blogs/future_tense/2012/09/28/darpa_plan_x_the_agency_wants_to_visualize_the_internet_for_cyberwarfare_.html
- http://gcn.com/articles/2012/08/22/darpa-plan-x-automated-tools-cyber-battle.aspx
- http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-cyberwarfare.html?pagewanted=2&hpw
- http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_print.html
- http://motherboard.vice.com/2012/8/24/ones-and-zeros-darpa-s-plan-x-dna-hard-drives-and-how-zynga-is-killing-soap-operas--2
- https://www.fbo.gov/utils/view?id=f69bba51a9047620f2e5c3a6857e6f6b

The NSA

Patrick Schultz

The Early Years

- Originally started as the Armed Forces Security Agency (AFSA) in 1949
- Established by the Department of Defense to be in charge electronic military intelligence and communication
- AFSA had little power and lacked organization. The organization had to be reworked.

Becoming The NSA

- Authorized in a Letter by President Truman 1952
- Existence was not acknowledge by the United States until 1970s.
- Technology advancements meant more power and money going to The NSA.

Overall Goal and Missions

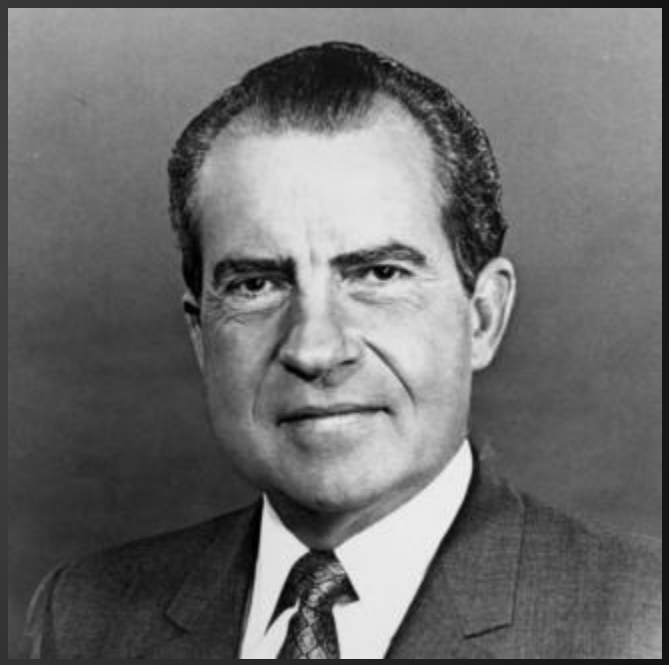
- Collect foreign data (radio broadcasts, web data, news media) for purposes of national security.
- Has limited control on digital information coming out of the country.
- Unlike the CIA, is more interested in finding out secrets than keeping them.

Headquarters

- Fort George G. Mead, Maryland
- Over 18,000 Parking Spots
- Additional facilities in Texas, Georgia and Utah

Controversies in recent years

- Nixon Wire Tappings - 1975
- Unconstitutionally wiretapping persons of interest
- Established Foreign Intelligence Surveillance Act



Data Security Programs

- ThinThread
- Trailblazer
- Turbulence

Warrantless Bush Wiretaps

- In 2005 President Bush filed an executive order to prevent terrorism
- Monitored phone conversations from all over the world, not just US. All without warrants.
- NSA argued it was within Bush's power.

Ethical Questions

- Privacy vs. Security?
- Too much power in one organization?
- Constitutionality?

References

1.http://www.nsa.gov/

2.http://www.archives.gov/research/guide-fed-records/groups/457.html

3.http://history.sandiego.edu/gen/20th/nsa.html

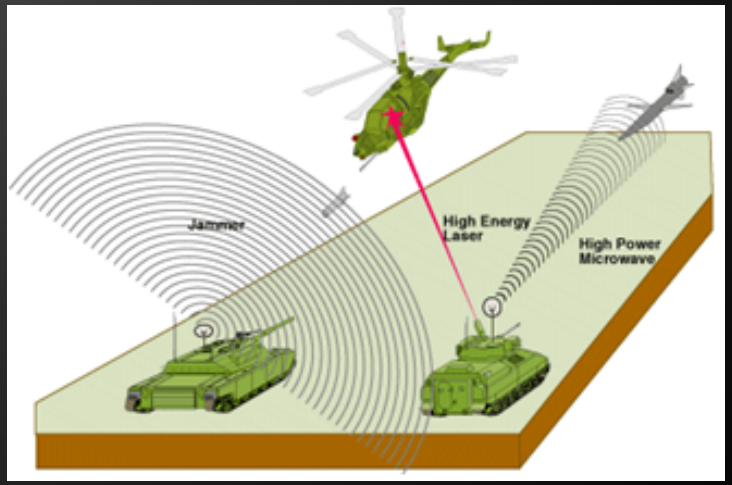
4.http://educatedearth.net/video.php?id=5189

Electronic Warfare

By Luke Schaumburg

What is Electronic Warfare?

- Electronic Warfare (EW) - refers to any action that involves using the electromagnetic spectrum or directed energy to control the spectrum, attack an enemy, or stop enemy assaults via the spectrum.
- Manipulation of radio waves, microwaves, sound waves, etc.
- Most often used in the military as an element of offensive and defensive counter-information
  (attack/defense on/of communication)



3 major subdivisions of EW

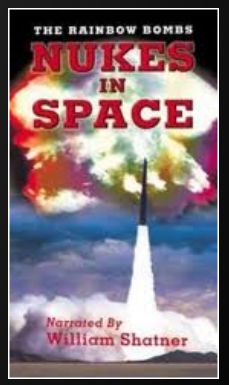
- Electronic Attack (EA) –
  - Communications jamming (interrupting radio or radar signals)
  - Directed energy (lasers, sonic weapons, particle beam projectiles)
  - flares, anti-air devices, EMPs (Electromagnetic Pulse)
- Electronic Protection (EP) –
  - flare rejection logic on IR missiles
  - “stealth” on planes
  - Protects from the effects of EA
- Electronic warfare Support (ES) –
  - pre-emptive threat recognition and prevention of EA

Electronic Warfare in History

- Russo-Japanese war of 1905: First consideration of using EW
- EW was used extensively in World War II in defending against and jamming radar and radio signals.
- Six Day War: the first modern day coordinated and integrated use of EW.
- Now days, EW is incorporated into the mainstream of all military operations and it would be inconceivable today to conduct any sort of military operation without planning EW activities.

Dangers of Electronic Attack

- Tampering with government security information
- Electronic power blackouts
- Terrorists with access to EW devices could wreak havoc on the general population, or governments, stealing or deleting information.
- It is thought that it would be possible to detonate a nuke in the mesosphere above the United States, which would cause an EMP blast powerful enough to wipe out almost all electronics in the country, leaving the American government “blind, deaf, and dumb.” according to an article in the Washington Post.
    - As of now, the US doesn't have a good defense for this, but the government is working on ideas.



Applications and possibilities

- interrupting communication lines
- EMP devices: anti-air
- Lasers: destroying missiles, artillery, rockets, and mortar rounds.
- "Microwave guns": heat up the water in a target's skin and causes incapacitating pain
- Sonic weapons: emits extremely high-powered sound waves that can disrupt or destroy the eardrums of a target and cause severe pain and disorientation. Used in counter-terrorist and crowd control situations.
- Pulsed energy projectile: emits an infrared laser pulse which stuns the target and causes pain and temporary paralysis. Under development and intended for crowd control.

Ethical issues/concerns

- Unseen effects from crowd-control devices like the pulsed energy projectile, or sonic weapons: could be a cause of cancer, permanent harm to eardrums
- Possibility of affecting the general population during military warfare.
- Any non-military use of EW devices used to cause harm, confusion, or power-outages poses ethical concerns.

References

- http://ew30.blogspot.com/2009/12/such-is-reliance-on-electromagnetic-em.html
- http://en.wikipedia.org/wiki/Electronic_warfare
- http://www.missilethreat.com/archives/id.16/subject_detail.asp
- http://en.wikipedia.org/wiki/Directed-energy_weapon

United States & Cyberspace

By: Tobi Schermuly

Questions?

- what should they do?
- what shouldn't they do?
- what do we want them to do?
- what can they do?
- what can you do?

what should they do?

President Obama has declared that the “cyber threat is one of the most serious economic and national security challenges we face as a nation” and that “America's economic prosperity in the 21st century will depend on cybersecurity.”

what shouldn't they do?

- affect us
- take away our privacy
- provoke attackers
- be ignorant
- jail time for hackers

what do we want them to do?

what can they do?

Near Term Actions

The President's Cyberspace Policy Review identifies 10 near term actions to support our cybersecurity strategy:

1. Appoint a cybersecurity policy official responsible for coordinating the Nation's cybersecurity policies and activities.
2. Prepare for the President's approval an updated national strategy to secure the information and communications infrastructure.
3. Designate cybersecurity as one of the President's key management priorities and establish performance metrics
4. Designate a privacy and civil liberties official to the NSC cybersecurity directorate.
5. Conduct interagency-cleared legal analyses of priority cybersecurity-related issues.
6. Initiate a national awareness and education campaign to promote cybersecurity.
7. Develop an international cybersecurity policy framework and strengthen our international partnerships.
8. Prepare a cybersecurity incident response plan and initiate a dialog to enhance public-private partnerships.
9. Develop a framework for research and development strategies that focus on game-changing technologies that have the potential to enhance the security, reliability, resilience, and trustworthiness of digital infrastructure.
10. Build a cybersecurity-based identity management vision and strategy, leveraging privacy-enhancing technologies for the Nation.

what can we do?

"When you cross the street, you look both ways to make sure it’s safe. Staying safe on the Internet is similar. It takes some common sense steps."

- organization
- work with DHS

References

http://stopthinkconnect.org/

http://www.whitehouse.gov/administration/eop/nsc/cybersecurity

http://www.dhs.gov/stopthinkconnect

http://www.dhs.gov/publication/stopthinkconnect-government-resources