“Cyber attacks...is not in any way comparable to weapons of mass destruction. What a lot of people call them is “weapons of mass annoyance.” If your power goes out for a couple of hours, if somebody draws a mustache on Attorney Gen. Ashcroft’s face on his website, it’s annoying. It’s irritating. But it’s not a weapon of mass destruction. The same is true for this”

~James Lewis, 2003, Director of the Center for Strategic and International Studies

Cyber-Warfare

Prof. Ing. Claudio CILLI
cilli@di.uniroma1.it
http://dsi.uniroma1.it/~cilli
Introduction to Cyber-Warfare

• **Cyberwar**
  • Leveraging the internet for political, military, and economic espionage activities

• **Cyberwarfare**
  • Politically motivated hacking to conduct sabotage and espionage

• **Dangers**
  • Lack of agreed upon definitions make preparation, defense, and response in the face of ‘attack’ difficult
  • The more developed a State is, the more dependent it is on the Internet
  • Internet is essential to every modern State
Cyber-Space – The Final Frontier

- Considered the newest domain of warfare
- Civilian vs. Civilian (Cyber-Crime)
- Civilian vs. State
- State vs. Civilian
- State vs. State
Cyberwar Myths (I)

- Small teams can do enormous damage
  - Best hope of a small team is $O(\$10b)$ in worm damage
    - Cannot target anything other than commonly available systems
    - Cannot manage broad testing of attacks
      - Only penetrate <10% of enterprise systems
  - Cannot seriously disrupt the economy
  - Takes large sophisticated institution to cause serious economic disruption
  - Only nation states can play at this level
Cyberwar Myths (II)

- Attacks in cyberspace can be anonymous
  - True at micro-scale of individual technological attack
  - Not true at macro-scale
    - Will be completely clear in grand strategic context who is conducting attack
    - Will be very large amounts of control traffic that will be hard to miss
      - 50,000 Chinese all doing *something* in US will get noticed
    - Attacker will generally *want* to be known
Cyberwar Myths (III)

- Cyberspace erases distance
  - Mobility is more like land/sea than air
    - Contrast to other thinkers
  - Battlefield is all information/knowledge
  - Expertise on disabling power turbines
    - Takes years to acquire
    - Is not instantly transferrable to, say, crippling bank’s transactional systems
  - Similarly defenders need deep understanding of the networks they defend.
  - First day on new network, will be pretty useless
    - True for attackers and defenders
Civilian Hackers

• Their threat-level ranges based on malicious intent
• Cyber-crime, not Cyber Warfare
  • Crime may be a step or signify the potential for individual hackers/collective hacktivists to participate in Warfare
• Documented Cases
  • 1970: MOD (Masters of Deception)
  • 2010: Spanish Investigators arrested 3 individuals responsible for BotNet infection of more than ½ of Fortune 1000 companies and > 40 major banks
Cyber War between Sunni vs. Shiite

“While media coverage focuses on the most high-profile hacks or defacements, this current cyber-campaign is a War of a Thousand Cuts…”

-Jeffrey Carr
*Inside Cyber Warfare*
Neo, The Matrix Has You

- “Anonymous”
  - Hacktivists
  - No central authority/hierarchy
  - Sheer size and capability poses threat
  - Capability, Opportunity, Intent... “not your personal army”

- Civilian vs. State can be far more dangerous than the petty annoyances that “Anonymous” may engage in
  - Operation Cast Lead (Israeli vs. Arabic Hackers)
One section that sticks out is Assange's discussion of the denial of service (DoS) attacks the site has managed to withstand.

From a translation of the interview:

SZ: Last week there was a hacker attack which paralyzed the WikiLeaks website with a Denial-Of-Service attack. How capable of action are you technical wise?

Assange: Our website is almost daily under attack. But we have developed enough countermechanisms to fight off such attacks.

SZ: Who's behind these attacks?

Assange: This ranges from mentally confused persons to governments.

SZ: Do you have evidence for that?

Assange: After our releases about China we witnessed attacks launched by Chinese government computers. Attacks on websites by governmental institutions however are a war crime, same as assaults on every other civilian infrastructure.

SZ: Is that enshrined in international law?

Assange: The international law is not that far yet.
Internet Policing

• “The U.S. reserves the right... to respond to serious cyber attacks with an appropriate proportional and justified military response.” – DepSecDef Lynn, Inside Cyber Warfare p.273

• International law makes response difficult and sensitive

• Asset-seizing, monitoring

• Foreign espionage vs. Sensitive personnel
  • GhostNet
    • U.S. Intelligence Community highly suspects GhostNet to be Chinese government
Cyber Attacks

• The Prussian philosopher Karl von Clausewitz observed: "Every age has its own kind of war, its own limiting conditions and its own peculiar preconceptions."

• We live in an age of TECHNOLOGY focused warfare
Definition

- Cyber Attacks: computer-to-computer attack that undermines the confidentiality, integrity, or availability of a computer or information resident on it
Lessons From Past Cyber Attacks

• Cyber attacks accompany physical attacks
• Cyber attacks are increasing in volume, sophistication, and coordination
• Cyber attacks are attracted to high-value targets
Physical Conflicts and Cyber Attacks

- The Pakistan/India Conflict
- The Israel/Palestinian Conflict
- The Former Republic of Yugoslavia (FRY)/NATO Conflict in Kosovo
- The U.S. – China Surveillance Plane Incident
Potential Cyber Attacks

- Unauthorized Intrusions
- Defacements
- Domain Name Server Attacks
- Distributed Denial of Service Attacks
- Computer Worms
- Routing Operations
- Critical Infrastructures
- Compound Attacks
Compound Attacks

- Employ some or all of aforementioned cyber attacks
- Possibly combined with conventional (physical) terror attack
- Consequences include devastating disruption in communication and commerce
Critical Infrastructures

- Critical infrastructures include gas, power, water, banking and finance, transportation, communications
- All dependent to some degree on information systems
- Insider threat - specialized skills
Potential Sources of Attacks

1. Thrill Seekers
2. Terrorist Sympathizers and Anti-U.S. Hackers
3. Terrorist Groups
4. Nation-States
Thrill Seekers

- No political motives
- Seeking notoriety – bragging rights
- “Nuisance attacks” using pre-fabricated tools and exploits
- Potential for serious disruptions and monetary damage
Terrorist Sympathizers and Anti-U.S. Hackers

• Extremist Muslim groups – known hacker groups (G-Force Pakistan, Pakistan Hackerz Club)
• Anti-Israeli groups
• Anti-capitalism and anti-globalization movement
• Chinese hackers

Pakistani Hackers Deface U.S. Site With Ultimatum

By Brian McWilliams, Newsbytes
KANSAS CITY, MISSOURI, U.S.A.,
17 Oct 2001, 9:44 AM CST

A Pakistani hacking group has defaced a Web server operated by the U.S. government and threatened to hit American and British military sites unless its demands are met.

A Web server operated by the National Oceanic & Atmospheric Administration (NOAA) was attacked this morning by a group known as GForce according to records at Alldas, a Web site defacement archive.

The attackers replaced the site's homepage with their own, which bore the title "GForce Strikes Back" and contained a 350-word text message. The message said the group would target "major U.S. military..."
Terrorist Groups

• Terrorist groups are using information technology
• Terrorists possess the will and may easily obtain the means to attack IT targets
• Potential for targeted cyber attacks is growing
Terrorist Groups: Multiple Data Points

- Attorney General Ashcroft, "Information found in an al-Qaeda safe-house detailing multiple American targets makes one thing clear: the terrorist enemies of our great nation recognize that attacks on such targets as nuclear power plants, chemical facilities, dams and internet hubs would strike at the heart of our critical infrastructures. If given the opportunity, these extremists would cripple America's information, financial, and utility systems. We must deny them such an opportunity."
Types of cyber warfare

• **Espionage and national security breaches**
  • Cyber espionage: the act or practice of obtaining secrets (sensitive, proprietary or classified information) from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers

• **Sabotage**
  • Computers and satellites that coordinate other activities are vulnerable components of a system and could lead to the disruption of equipment.

• **Denial-of-service attack**
  • A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers.
Targets of Cyber Warfare

- The spectrum is very wide. In general a cyber weapon could hit every critical infrastructure and vital system of a country such as:
  - Industrial control systems, of particular concern are those components that oversee the operation of plants for energy production and delivery of services of various kinds, such as water utilities.
  - Electric power supply grids.
  - Systems for territory controls.
  - Hospitals and government controls.
  - Communications networks.
  - Defense systems.
  - Military air traffic and airspace control systems.
  - Financial and banking systems.
Electrical power grid

• U.S. Government: Admitted the electric power transmission is susceptible to cyber warfare.
• Dept. of Homeland Security working with the industry to:
  • 1. Identify vulnerabilities
  • 2. Enhance the security of control system networks,
  • 3. Ensure that security is built in the next generation of "smart grid" networks
• April 2009: According to current and former national security officials: China and Russia had infiltrated the U.S. electrical grid and left behind software programs that could be used to disrupt the system,
• Project Aurora and Cyber Warfare
• https://www.youtube.com/watch?v=RmD9HY8L9h8
Stuxnet

- Computer worm discovered in June 2010
- Is thought to be created by the United States and Israel to attack Iran's nuclear facilities.
- Distributed with thumb drives and spreads via Microsoft Windows, and targets Siemens industrial software and equipment.
- First discovered malware that spies on and subverts industrial systems.
- Initially spreads indiscriminately
- Includes a highly specialized malware payload that is designed to target only Siemens supervisory control and data acquisition (SCADA) systems that are configured to control and monitor specific industrial processes.
Recent cyber attacks

• Last six weeks: 15 banks offline for a total of 249 hours (denial of service cyber attacks). Possibly Iran is behind the attacks as retaliation for an online video mocking the Prophet Muhammad. Intended to interrupt accounts, not to hack information.

• Spamhaus listed Cyberbunker as hosting spam. Cyberbunker retaliated with denial of service attack to Spamhaus, causing internet speeds to slow, Netflix being one of the major companies suffering from it.
Rules of Cyber Warfare

• Tallinn Manual on the International Law Applicable to Cyber Warfare analyzes the rules of conventional war and applies them to state-sponsored cyber attacks. Created at the request of NATO and is a proposed set of rules for how international cyber warfare should be conducted
• Written by 20 experts in conjunction with the International Committee of the Red Cross and the US Cyber Command
• The manual advises that attacks must avoid targets such as hospitals, dams, and nuclear power stations in order to minimize civilian casualties
• It's acceptable to retaliate against cyber attacks with traditional weapons when a state can prove the attack lead to death or severe property damage
• It also says that hackers who perpetrate attacks are legitimate targets for a counterstrike (Basically, it’s ok to kill hackers now)
“Sample Nuclear Launch While Under Cyber Attack”
The Bombs Bursting in... Binary?

- State – State
  - Some state-sponsored organizations that engage civilians can also engage states; the difficulty being the “return address problem”
  - Ambiguity halts any linkage between state and non-state actor sponsorship; therefore forbidding war based on international law
- State vs. Iran (StuxNet)
  - Either Israel or U.S. implanted a worm in Iranian nuclear-facilities
- United States vs. Libya
  - U.S. discussed using cyber-attacks to cripple Libyan infrastructure
Evolution of War

- Most Dangerous Cyber Attacks
  - Modernized countries are most vulnerable to these attacks
- The Need to Evolve
  - For security to be more effective, offensive advancements necessitate defensive advancements
  - Over last 5 years, 650% increase in security breaches...USGAO Report to Congressional Committees

*This figure represents a projection based on incidents logged from January 1, 2010, to June 30, 2010. The projection assumes a constant rate of malicious activity throughout the year.*

Sources: U.S.-China Economic and Security Review Commission, Hearing on China’s Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities, testimony of Gary McKinnon, May 29, 2008; Name withheld (staff member, U.S. Strategic Command), telephone interview with Commission staff, August 21, 2009; Name withheld (staff member, U.S. Cyber Command), e-mail interview with Commission staff, August 17, 2010.
Relevant Expertises

- Network security
- Network ops
- Cryptography
- IDS
- Vulnerability Assessment
- DDoS
- Worm defense

- Economics
- Management Science
- Organizational Psychology

- Military Strategy
- Military History

No-one is an expert in all of these...
Five Levels of Strategy

- Due to Luttwak, Liddell-Hart
- Technological
  - Iron swords, longbows, railroads, aircraft, tanks...
  - Exploits, DDOS, worms, firewalls, IDS...
- Tactical
  - Tanks in formation (WWI/WWII), longbows in dismounted ranks behind stakes (Crecy, Agincourt)
  - What we do with a DDOS tool, or an IDS?
Five Levels of Strategy

• Operational (individual battle level)
  • Waterloo, Crecy, Midway, Carshemish
  • Individual organization (utility, bank, ISP, carrier battle group)

• Theatre Strategy
  • WWII: Pacific, European, North African
  • Cyberwar same (but opens new theatres for attack)

• Grand Strategy
  • National level strategy - decisive military defeat, economic exhaustion, nuclear blackmail, erosion of will
How Many Operations in Theater

- Have to pick enough companies/organizations
- That infrastructures can’t function except in small pockets
- SWAG: $O(100)$ largest energy companies
- Simultaneous surprise attacks on them
- Forces required are 100x forces for one
- Now move down to operational level
Is the Vulnerability There?

- Almost certainly
- SCADA done over IP/Windows these days
- Developers not used to a hostile environment
  - Labor in obscurity
- So just about certain to be plenty of vulnerabilities
- Machinery trusts its control system to look after it
Is the Attack Trivial Then?

• Could a small band of hackers pull this off?
• No!
• Huge amounts of obscurity
• Great diversity in SCADA systems
  • Need vulnerabilities in most of them
  • Lots of testing needed
  • No public community working on this to help
• Great diversity in deployments
  • Which IP range is power station XYZ?
• Attackers know none of this ab-initio
  • Either reconnoiter up front
  • Or find out on fly
Attacker Information Needs

• For each of O(100) operational targets, need
  • Fairly detailed map of network/organization
    • What assets are where on network?
    • What software is in use for most critical purposes?
      • Brand/version
    • Where defenders are?
    • Where key operational execs are?
  • To have developed vulnerabilities
    • For all key software systems in use
    • Requires being able to get copies of them
      • Pretend to be a customer
Advance Reconnaissance Options

• Insiders
  • Get spies jobs as (preferably) IT staff
  • Over time, stealthily map network and organization
  • Ideally want several in different areas for 1-2 yrs
  • Gives layer 8 view

• Cyber-surveillance
  • Remotely compromise some desktops internally
  • Use them to map network at layer 2-7
  • Capture keystrokes etc.
  • Must be stealthy and untraceable
    • No Chinese strings in Trojan
    • Communication path home must be convoluted
Cyber Battalion (1 operation)

- **Command (6)**
  - Reconnaissance/Planning
    - Advance Rec (6)
    - Battle mapping/ Situational Awareness (12)
    - Detailed Battle Plans (6)
    - Outside Damage Assessment (3)
  - Operations
    - Backdoor Access (10)
    - Defense suppression (20)
    - Offensive operations
      - Group 1 (10)
      - Group 2 (10)
      - Group 3 (10)
      - Could be tens of these
  - R&D
    - Vulnerability Research (10)
    - Scripts and Tools (10)
  - Logic Bombs

Could be tens of these
During Attack

• All major teams must deploy quickly from small beachhead
  • Backdoor team (highest priority)
    • Compromises utility systems for other teams to use
    • Installs backdoors, remote dial-ups, etc. to get back in later
    • Owns RAS servers, access routers etc.
    • Preferably 100s-1000s of systems so every system in enterprise must be thoroughly cleaned
  • Defense Suppression Team
    • DOS, disabling, and destruction of systems used by defenders
    • Firewalls, IDS’s, desktops and laptops used by sysads
  • Offensive operations groups
    • Cripple actual infrastructure assets (turbines, pumps, etc., etc.)
    • Physical damage where possible,
    • Disable/corrupt control systems
  • Logic bomb group inserts logic bombs in many systems and turns them off
Balance of Force in operations

• Attackers: 150-1000 attackers
• Defenders (today):
  • Security group: 1-10
  • Network group: 10-20
  • End-host sysads: 100s-1000s
• Attackers have
  • surprise,
  • superior organization
• Defenders
  • know terrain better
  • Have physical access (sort of)
• Could your organization survive this kind of assault?
Defense Response (today)

• Reboot the company
  • Disconnect from network
  • Turn everything off
  • Unplug every phone cable
  • Bring things up and clean and fix them one at a time
• A single Trojan left untouched lets attacker repeat the performance
• Likely to take weeks
• Cannot have confidence that we fixed all the vulnerabilities the attacker knows
Attacker Requirements

• Discipline, training
• **Hard** to get hundreds of people to execute a complex plan.
  • Everyone must understand the plan
  • Everyone must be extensively trained on tactics/technology so it’s second nature
  • Must follow plan and replans flawlessly
  • And yet be creative enough to improvise
    • “Plan never survives contact with the enemy”
    • “Fog of War”
  • These issues have always been critical in military operations
• And have to repeat this for $O(100)$ simultaneous operations
Defensive Implications

- The networks of critical organizations will need to be run as a military defense at all times.
  - Constant alertness
  - Well staffed
  - Regular defensive drills
  - Standing arrangements for reinforcement under attack
  - Extensive technological fortification
  - Excellent personnel and information security
Preventing reconnaissance

• An attacker who can develop a detailed well-informed plan at leisure will win.
  • Personnel security
    • Background checks for power company staff should be
    • Comparable to security clearances for military/intel
  • Prevent scans
  • Critical information is on a need-to-know basis
  • (Turbine manuals are not on internal web)
  • Extensive internal deception/honeynet efforts
    • Reconnaissance will find all kinds of bogus things
• Force attack to be extemporized
Implications

- Defending nation in cyberspace is a **military** problem
- Will require militarizing critical infrastructures.
- Will require new paradigms and tools
- Critical infrastructure is in private hands
- Huge tension – not a good outcome for civil society
- Deeply ironic that this is result of network promoting openness
- Luttwak’s “Paradoxical logic of strategy”
Defacements Don’t Need to Be “Dramatic”: A Few Words Are Enough to Prove That A Breach Happened And That Remediation Will Be Needed

<table>
<thead>
<tr>
<th>Mirror saved on: 2008/05/15 23:16</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Defacer:</strong> ISCN</td>
</tr>
<tr>
<td><strong>Domain:</strong> <a href="http://namru3.med.navy.mil/Portals/0/ISCN.txt">http://namru3.med.navy.mil/Portals/0/ISCN.txt</a></td>
</tr>
<tr>
<td><strong>IP address:</strong> 205.73.217.15</td>
</tr>
<tr>
<td><strong>System:</strong> Win 2003</td>
</tr>
<tr>
<td><strong>Web server:</strong> IIS/6.0</td>
</tr>
<tr>
<td><strong>Attacker stats</strong></td>
</tr>
</tbody>
</table>

Owned By: Magic-Boy And Imm02tal
Contact Us: ISCNltd@GMail.com
ISCN Team
Some Defacements, However,

[Image of defaced website content]

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

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

Terrorist Crew

~ Hi Master ~

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

Gratz to: Kerom135, GoX, Oscar-Sandos, CoRR@il, The BokiR, el-CR
Decomposing A Web Site Defacement

- A web site defacement consists of four key elements:

  1) A system with a vulnerability is identified and exploited, allowing unauthorized access by a malicious third party.

  2) Existing web pages are modified or replaced with new text or graphics, or a web server and content of the attacker’s choice is installed (if the system didn’t already have a web server on it).

  3) The modified site is publicized/confirmed by an independent third party.

  4) Something happens (or not). What is it that an attacker might hope to accomplish as a result of a web site defacement?
“Cyber War” In Estonia, 2007

• Remember this one? It sure got a lot of press coverage!

Estonia hit by 'Moscow cyber war'

Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.

Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.

Estonia says the attacks began after it moved a Soviet war memorial in Tallinn. The move was condemned by the Kremlin.
But What *IS* A “DDoS” Anyway?

• In a distributed denial of service attack, or DDoS, an online service (such as a web site) is flooded with bogus traffic, thereby keeping real users from using the service.

• In Estonia’s case, they suffered a fairly classic DDoS attack: government web sites, media web sites and other Estonian web sites were flooded with unsolicited network traffic, thereby making those web sites effectively unusable for their intended purpose until the attacks stopped or were mitigated.
Some People, Including Estonia Itself, Eventually Had Doubts About This "Cyber War"


• Gary Warner, ‘Evidence that Georgia DDOS attacks are “populist” in nature,’ http://garwarner.blogspot.com/2008/08/evidence-that-georgia-ddos-attacks-are.html

Punishment for “Cyber War”: Less Than $2,000

Estonia fines man for 'cyber war'

A 20-year-old ethnic Russian man is the first person to be convicted for taking part in a "cyber war" against Estonia.

Dmitri Galushkevich was fined 17,500 kroons (£830) for an attack which blocked the website of the Reform Party of Prime Minister Andrus Ansip.

The assault, between 25 April and 4 May 2007, was one of a series by hackers on Estonian institutions and businesses.

At the time, Estonia accused the Russian government of orchestrating the attacks. Moscow denied any involvement.
Another Recent DDoS Example: Georgia

Monday, 11 August 2008

Georgian Websites Under Attack - DDoS and Defacement

The Attacks Resume

Last month we had reported on a crippling distributed denial of service (DDoS) attack against Georgian President Mikheil Saakashvili's website. Shortly after the blog the command and control (C&C) server used to issue these attacks was taken offline. We have not seen the C&C come back to attack any other websites. In fact we had not seen any other C&C servers taking aim at Georgian websites since that blog until last Friday (August 8, 2008). The date appears to coincide with military movement that has since escalated into fighting between the two countries. Since August 8 we have witnessed multiple C&C servers attacking websites that are Georgian or sympathetic to the country.

Some of the first targets we saw once again involved the Georgian government. The website for the President (www.president.gov.ge) and the website for the Parliament of Georgia (www.parliament.ge) were both targeted. However, the attacks were not limited to just government websites. We have witnessed at least six different C&C servers attacking various websites that are not government sites. In some cases the various C&C servers were and still are attacking the same websites. The following websites have come under attack in the past few days:

www.president.gov.ge
www.parliament.ge
apsny.ge
news.ge
tbilisiweb.info
newsgeorgia.ru
os-inform.com
www.kasparov.ru
hacking.ge
mk.ru
newstula.info
skandaly.ru
“Georgia Cyberwar Overblown”

- **There are two problems with the theory of cyberwarfare in the Caucusus.** The first is that all of the reported attacks consisted of DoS against Web sites, mostly connected with government functions. There were no reports of attacks against critical infrastructure, electronic jamming of stock exchanges, SCADA-hack explosions in substations or anything like that. This was not a battalion of elite army-trained hackers from the Russian Southern Command of Cyber Warfare (Unit 1337). In all likelihood it was groups of run-of-the-mill script kiddies with control of a botnet, stroking their egos with the higher cause of injured nationalism. More "Boris waz ere" than "All your SCADA are belong to us."

- **The second problem is that in order for cyberwarfare to be successful there needs to be a lot of cyberinfrastructure to attack.** Georgia and Russia are both making tremendous strides in development of Internet infrastructure but let's not kid ourselves. These are not info-economies running all their banking in virtual reality on top of Second Life. The targets that were attacked were mostly government brochure-sites. **Even in the United States, where a lot of government services are delivered over the Web, a sustained DoS attack against government Web sites would not really affect the economy. It would simply make the online experience more like the real-life DMV experience, and we somehow survived that fine up to 1995.**

BEIJING, April 16 -- China is demanding an apology from CNN for broadcasting malicious remarks. A commentator on the US news channel called the Chinese "goons" and labelled their products "junk."

"We're running hundreds of billions of dollars worth of trade deficits with them, as we continue to import their junk with the lead paint on them and the poisoned pet food. I think they're basically the same bunch of goons and thugs they've been for the last 30 years."

Jack Cafferty made the comments earlier this month on CNN's political program, the Situation Room. Chinese Foreign Ministry spokeswoman Jiang Yu says China is shocked at the slander and strongly condemns such an evil attack on the Chinese people.

Jiang Yu, spokeswoman of Foreign Ministry of China, said, "Cafferty used the microphone in his hand to slander China and the Chinese people, and seriously violated reporting ethics. His remarks reflected his arrogance, ignorance and hatred towards the Chinese people. Such remarks have sparked strong indignation among Chinese people at home and abroad, and will certainly incur condemnation by people who safeguard justice all around the world. We solemnly request CNN and Cafferty himself to take back his malicious remarks and apologize to all Chinese people."

Overseas Chinese in the United States have launched an online campaign for apology from CNN and Cafferty. The petition has approximately 8,000 names.

(Source: CCTV.com)
“The Perfect Attack”

• You may be inclined to laugh when you hear me say this, but spam is, in many ways, the “perfect cyber warfare weapon.”

• Heck! I’m pretty sure that most of you don’t even believe that spam is a weapon. Spam is a low intensity, diffuse, and persistent “annoyance,” and not a sudden, high intensity, concentrated and dramatic frontal attack. So how could such a “trivial” thing be an “attack?” Wouldn’t we know it if we were being attacked?

• Maybe not. Because we’ve been suffering from spam for thirty years now, and because spammers have only gradually “turned the heat up over time,” we’ve all become accustomed to spam, and we’ve all gradually developed an increasing tolerance for more and more and more of it.

• Most of us don't even have a sense of how much spam is actually being sent out there – do you?
BILLION Spam/day <= 200 BILLION Spam/day

<= 11.4% Legitimate Email
How Much Does Spam Cost the US Economy?

- The total costs depends on what you “count:”
- lost productivity as staff spend time reading or deleting spam?
- costs associated with "false positives" (e.g., missed business deals caused by mis-filtering crucial messages as spam)?
- additional storage and processing power required to cope solely with spam-related traffic
- cost of anti-spam software or anti-spam hardware?
- costs to ISPs as they struggle to help infected customers get cleaned up after getting their PCs turned into spam zombies?
- consumer losses associated with spam scam fraud including non-delivery of merchandise, or delivery of fake products?
  - -- forgone sales due to spamvertised counterfeit/knock-off/pirated merchandise (pillz, watches, software, music, movies, etc.)?
  - -- medical and social costs associated with online sale of scheduled controlled substances (narcotics, steroids, etc.) (n.b. over 80% of all Storm worm spam is pharma-related)
One (Low) Estimate of Spam’s Costs

- "Ferris Research estimates that spam will cost $140 billion worldwide in 2008, of which $42 billion will be in the United States alone. If you compare these numbers with Ferris’s 2007 estimates of $100 billion and $35 billion, you’ll see that the cost of spam has increased substantially over 12 months."
- That $42 billion dollar estimate is obviously a lot of money, and if anything, I suspect that number is low. So why aren't people noticing those costs? Answer: it is being taken from us in little tiny nearly immeasurable pieces, billions of times a day, from people all across our country: $42,000,000,000 / 301,139,947 people / 365 days per year= "just" $0.382 per American per day, or $11.46/American/month
For Comparison, Some Other Recent Costs


- "In February 2008, the Congressional Budget Office projected that additional war costs from FY2009 through FY2018 could range from $440 billion, if troop levels fell to 30,000 by 2010, to $1.0 trillion, if troop levels fell to 75,000 by about 2013. Under these scenarios, CBO projects that funding for Iraq, Afghanistan and the GWOT could reach from about $1.1 trillion to about $1.7 trillion for FY2001-FY2018.”

- The Cost of Iraq, Afghanistan, and Other Global War on Terror Operations Since 9/11, Updated July 14, 2008, CRS Report RL33110, page 2
So What Might It Cost a Foreign Power To Wage A Cyber War? Nothing...


- In contrast to failed US efforts, both China and Russia have adopted the OSW [Open Source Warfare] approach to cyberwarfare. How did they do it? Simply:
  - Engage, co-opt, and protect cybercriminals. Essentially, use this influence to deter domestic commercial attacks and encourage an external focus. This keeps the skills sharp and the powder dry.
  - Seed the movement. Once the decision to launch a cyberattack is made, start it off right. Purchase botnets covertly from criminal networks to launch attacks, feed 'patriotic' blogs to incite attacks and list targets, etc.
  - Get out of the way. Don't interfere. Don't prosecute participants. Take notes
And Spam Enables Many Other Corrosive Attacks on America

• For example, among the most persistently spamvertised products are scheduled controlled substances, e.g., prescription drugs which are distributed without a valid prescription
• How many new addicts have been created as a result of easy online access to prescription narcotics and other dangerous drugs?
• What is the cost to our country associated with the lives destroyed by easy online access to addictive substances?
• How much crime occurs as addicts, desperate to buy more drugs, commit robberies or burglaries, shoplift merchandise, engage in street prostitution, or engage in carding, phishing, or other crimes?
• And what sort of nefarious activities get funded with the money that's sent to these drug dealers overseas?
Preparing for a Cyber Attack

Countdown to eDay!
A Recent Poll

How prepared is the U.S. for a cyber attack?

43% Not Prepared
47% Somewhat Prepared
10% Very Prepared

Source: A collaborative effort between DefenseTech.Org and the Technolytics Institute with nearly 1,000 respondents to the poll.
Impact of a Cyber War

The political fallout of a cyber attack will be high, but this will pale in comparison to the financial and economic impact!

The financial and economic impact could be as high as $30 billion a day!
Impact of a Cyber War

That’s $425 million a day.
Cyber Media Warfare

One can only imagine the psychological impact on the viewers that witnessed this prank. The TV channel CT2 said that they received frantic phone calls from viewers who thought a nuclear war had started.

http://www.youtube.com/watch?v=MzaN2x8qXcM
Think About This

- What if the Internet went away:
  - For a day
  - A week
  - A month
- No eMails
- No BlackBerrys
- No eCommerce

Virtual business services of all sorts, accounting, payroll and even sales would come to a halt, as would many companies.
The worst thing to do -

• There is no doubt today that VoIP is taking over the telecom market, and every month increases penetration into business, government and the consumer sectors
  • Almost two-thirds of large organizations in North America will be using VoIP products and services by year end
  • Small Business VoIP adoption will grow to 3 million by 2010. Revenues are projected to reach $2 billion.
  • Consumer VoIP adoption will drive wholesale VoIP revenues to $3.8 billion by 2010

You are putting all your eggs in one basket.
Cyber Weapons Proliferation

- The cost to develop this new class of weapon is within reach of any country, any extremist group, any criminal organization and tens-of-millions of individuals. The raw materials needed to construct cyber weapons are not restricted and are widely available. We now have a weapon that can strike at the speed of light, it can be launched from anywhere in the world, and it can target anywhere in the world. This briefing will provide an understanding of the current state of cyber weapons, current defenses and a unique look at what the future cyber warfare scenario might encompass.
Modern Weapons Economics

What does a stealth bomber cost? $1.5 to $2 billion

What does a stealth fighter cost? $80 to $120 million

What does an cruise missile cost? $1 to $2 million

What does a cyber weapon cost? $300 to $50,000
Find the Weapons Facility

Nuclear Weapons Facility

Cyber Weapons Facility

Where’s the Cyber Weapons Facility?
In one year, between 2006 and 2007, there was a substantial increase in the number of countries pursuing cyber weapons.

After analysis of available information, we have concluded that in 2008 there will be over 140 countries with cyber weapon programs.
Cyber Arms Dealers

• RBN and their support units provide scripts and executables to make cyber weapons undetectable by antivirus software. Every time a copy of the cyber weapon is generated, it looks different to the anti-virus engines and it often goes undetected. The modularization of delivery platform and malicious instructions is a growing design in cyber weapons. RBN’s cyber weapons are very popular and powerful. In June 2007, one was used by a single person to attack and compromise over 10,000 websites in a single assault.

Did you know RBN leases use/capacity on their 150 million node BotNet?
Cyber Weapons Evolution

- Basic Weapons
- Advanced Weapons

Timeline:
- 1994
- 1998
- 2002
- 2004
- 2008
- 2012
- 2016

Legend:
- Basic Research
- Applied Research
- Early Adopters
- Rapid Advancement
- Significant Threat
• NATO's cyber defense chief has warned that computer-based terrorism poses the same threat to national security as a missile attack. He went on to say that “Cyber war can become a very effective global problem because it is low-risk, low-cost, highly effective and easily globally deployable. It is almost an ideal weapon that nobody can ignore.”

• Using this as a framework, we can put into context the evolving architecture for cyber weapons
Cyber Weapons Design

- **Cyber Weapon Architecture**
- A missile is comprised of three basic elements. The first is a delivery vehicle (rocket engine), followed by a navigations system (tells it how to get to the target) and finally the payload (the component that causes harm). As it turns out, the same three elements now appear in the design of cyber weapons.
Cyber Weapons Design

- **Cyber Weapon – Delivery Vehicle**
- There are numerous methods of delivering cyber weapons to their targets. Emails with malicious code embedded or attached is one mechanism of delivery. Another delivery vehicle is web sites that can have malicious links and downloads. Hacking is a manually delivery vehicle that allows a cyber soldier to place the malicious payload on a target computer, system or network. Counterfeit hardware, software and electronic components can also be used as delivery vehicles for cyber weapons.
Cyber Weapons Design

- **Cyber Weapon – Delivery Vehicle**
- Just as a navigation system guides a missile, it allows the malicious payload to reach a specific point inside a computer, system or network. System vulnerabilities are the primary navigation systems used in cyber weapons. Vulnerabilities in software and computer system configurations provide entry points for the payload of a cyber weapon. These security exposures in operating systems or other software or applications allow for exploitation and compromise. Exploitation of these vulnerabilities may allow unauthorized remote access and control over the system.
Cyber Weapons Design

• **Cyber Weapon – Delivery Vehicle**
• The payload of a missile is sometimes called a warhead and is packed with some type of explosive. In a cyber weapon the payload could be a program that copies information off of the computer and sends it to an external source. It can also be a program that begins to ease or alter information stored on the system. Finally, it can allow remote access so that the computer can be controlled or directed over the internet. A “bot” (a component of a botnet) is a great example of a payload that allows remote use of the computer by an unauthorized individual or organization.
Cyber Weapons Design

• **Cyber Weapon – Architecture**
  • This three element architecture demonstrates how advanced and sophisticated cyber weapons are becoming. The architecture creates reusability and reconfiguration of all three components. As one software or system vulnerability is discovered, reported and patched, that component can be removed and replaced while the other two components are still viable. This not only creates flexibility but also significantly increase the productivity of the cyber weapons developers.
Questions?