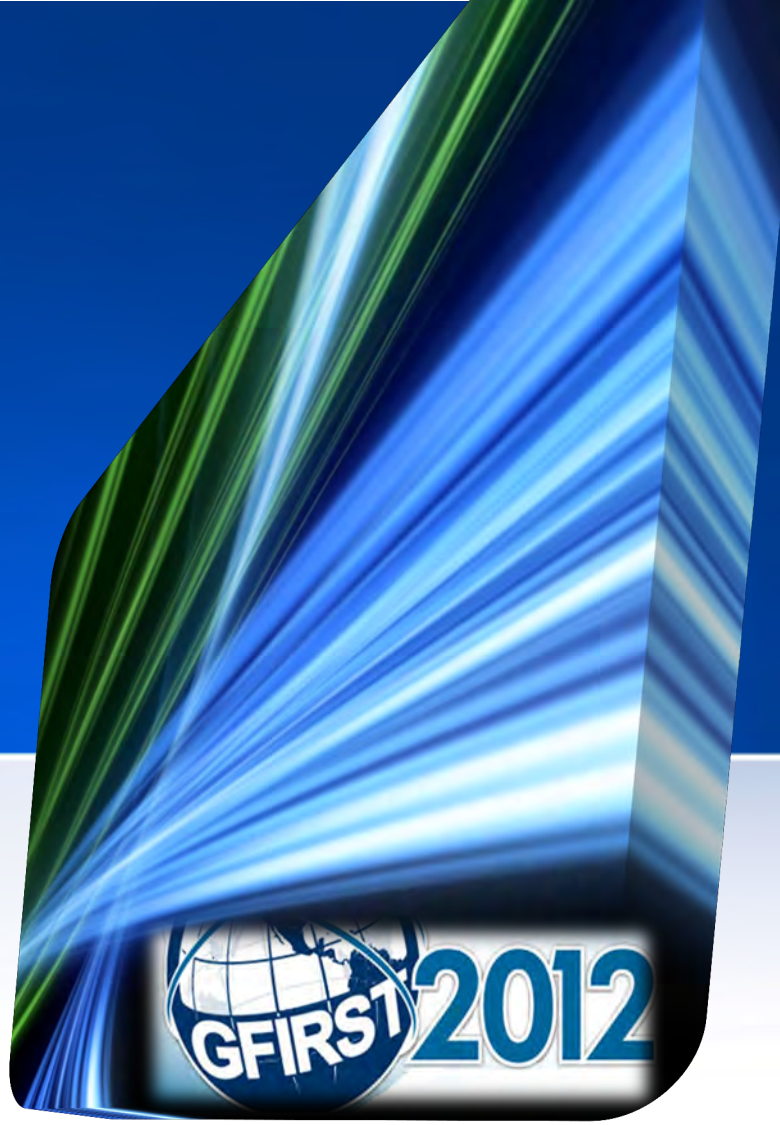
ARE WE *REALLY IN A CYBERWAR? THE DANGERS OF HYPE*



Dr. Julie E. Mehan, PhD

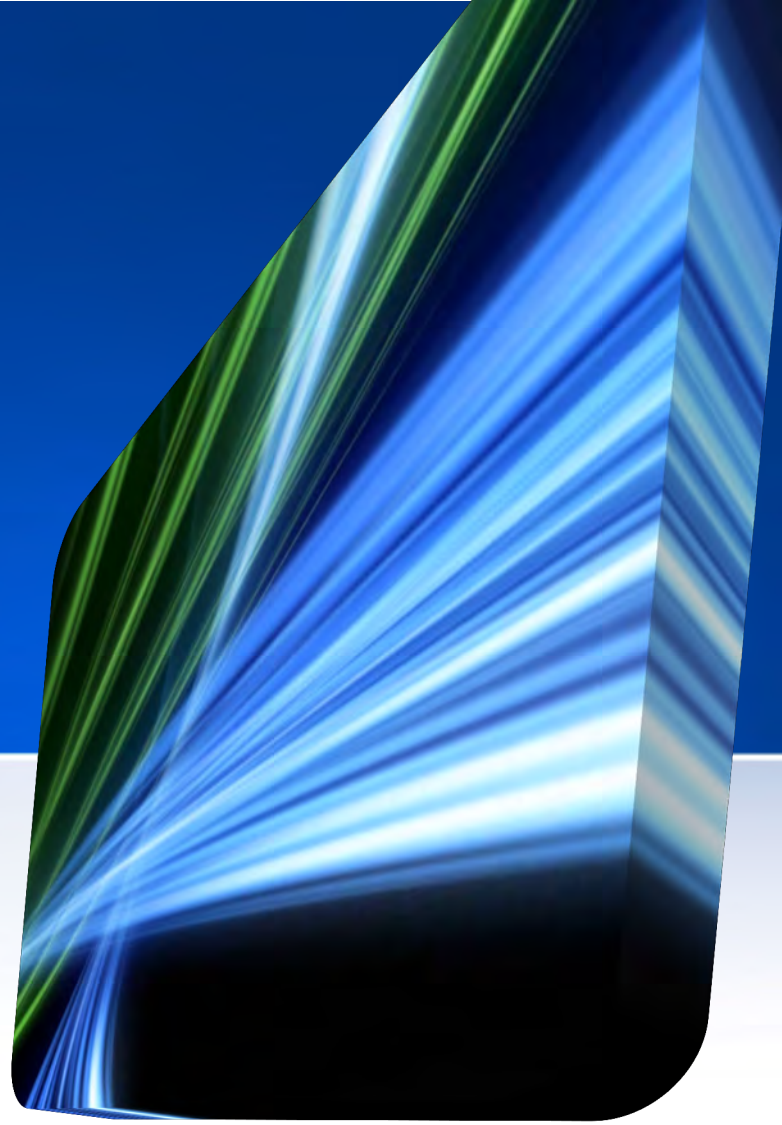
8/3/2012

School of Cyber Security

LUNARLINE

This Is A Controversial Topic

- Richard Clarke, the former special advisor to the president on cybersecurity, has broadly claimed that any attempt to penetrate computer systems constitutes cyber war.
- But Howard Schmidt, the most recent cybersecurity czar, has gone as far as saying that cyber war does not exist – since digital attacks fall short of any reasonable definition of war.



DEFINITIONS: LET'S AGREE ON VOCABULARY

Let's Start with a Definition of War

- Merriam-Webster: "War is an organized, armed, and often a 'prolonged conflict' that is carried on between states, nations, or other parties typified by extreme aggression, social disruption, and usually high mortality."
- Military general and theoretician Carl Von Clausewitz defined war as follows: "War is thus an act of force to compel our enemy to do our will."

Definition of Cyberwar

- "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"
- "… a new domain in warfare" – William J. Lynn, U.S. Deputy Secretary of Defense
- "…the use of force in cyberspace." – Duncan Hollis, Professor of Law, Temple University

Relationship to Traditional Warfare

- CyberWar could be additional domain in traditional warfare
  - Used as initial stage to reduce command and control facilities, harm national infrastructure, spread propaganda, reduce confidence in government
- Could be a standalone approach to warfare
  - Potential for significant harm in the information age
- Increasingly difficult to distinguish countries and organizations
  - Countries may be (increasing evidence that they are) using 3rd parties (organized crime, other organizations) to do their work

Is the Term "Cyberwar" Appropriate?

- Nature of warfare has changed
  - WW II => Vietnam => Iraq / Afghanistan
- Does the term overstate or misstate the issue?
  - Where is the line between war and espionage, war and terrorism, or war and crime (e.g. theft)?
    - These definitions are blurred as the actions are converging.

CyberTerrorism

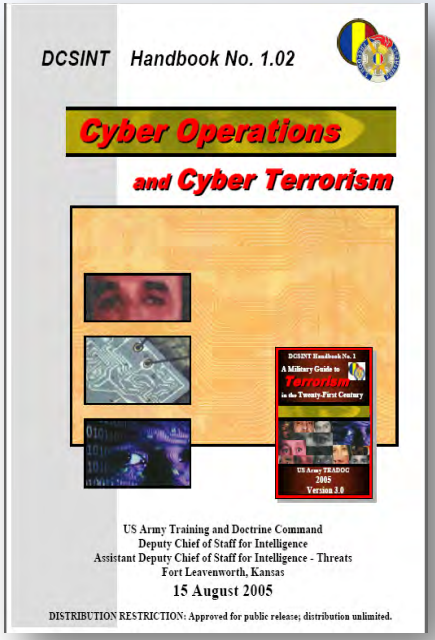
- **CyberTerrorism**
  - actions by terrorists to penetrate another nation's computers or networks for the purposes of causing damage or disruption
  - Characteristics of CyberTerrorism:
    - The act must have must have *scale* and *publicity*
    - Cyberterrorism is safe and profitable
    - Cyberterrorism is difficult to counter without the right expertise and understanding of the Cyberterrorist's mind.
    - Relatively anonymous

Characteristics of CyberTerrorism

- Unlike other acts of terrorism, if the CyberTerrorist loses today, he/she does not die – he/she learns what did not work, and will use that information against you tomorrow.

CyberWarfare & CyberTerrorism

- Cyber Warfare and Terrorism are also called asymmetric warfare.
  - CyberWarfare & Terrorism
    - "The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives."



Source: U.S. Army Cyber Operations and Cyber Terrorism Handbook 1.02

CyberEspionage

- **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
  - Unauthorized probing to test a target computer's configuration or evaluate its system defenses, or the unauthorized viewing and/or copying/theft of data files

Intellectual Property

- "Senior representatives from the intelligence community told us that they had conclusive evidence, covertly obtained from foreign sources, that U.S. companies have lost billions in intellectual property."
  - Carnegie Mellon, Center for International and Strategic Studies, February 2011

CyberCrime

- Cyber-Crime:
  - "..a crime committed where the use or knowledge of computers is required".
  - (e.g., denial of service, attacking passwords)
- Computer-assisted Crime:
  - "a crime in which the computer is used to assist in perpetrating the crime".
  - (e.g., fraud, child pornography)

Hacktivism

- Hacktivism is hacking with a cause and is concerned with influencing opinions on a specific issue.
- Example: ELF hacks into the web page of a local ski resort and defaces the web page. This is done to reflect the groups objections to environmental issues.

Source: ABC

Advanced Persistent Threats (APT)

- APTs are focused on gaining control of crucial infrastructure, such as power grids and communication systems. APTs also target data comprised of intellectual property and sensitive national security information.
  - It's automated, but on a small scale. Automation is used to enhance the power of an attack against a single target, not to launch broader multi-target attacks.
  - It's one layer. One party owns and controls all hacking roles and responsibilities.
  - It's very personal. The attacking party carefully selects targets based on political, commercial and security interests. Social engineering is often employed.
  - It's persistent. If the target shows resistance, the attacker will not leave, but rather change strategy and deploy a new type of attack against the same target.

Source: Amichai Shulman

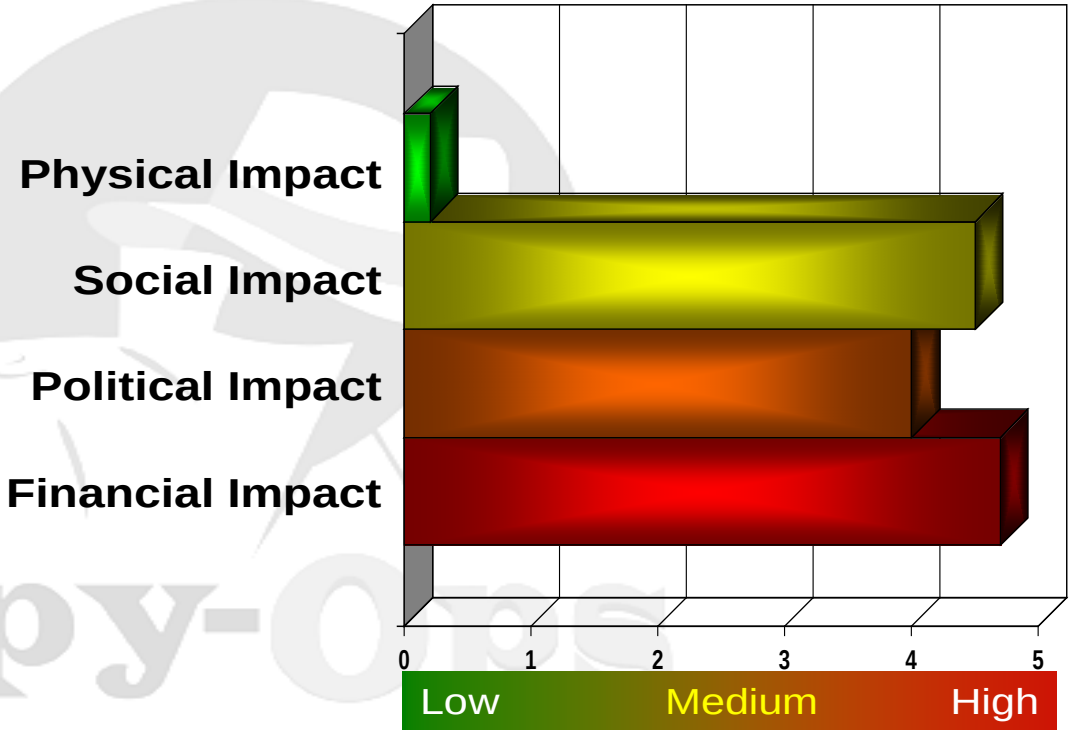
Impact of a Cyber War

INTELLIGENCE BRIEFING

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!



Overstating the Threat

- Is the threat of Cyberwar overstated?
  - Several experts say yes, including Marc Rotenberg (Electronic Privacy Information Center) and Bruce Schneier (Chief Technology Officer, BT Counterpane)
    - Much hyperbole, “sexy” news
    - Little distinction by many between cyber warfare and cyber spying; significant threats today from cyber-espionage
    - Used to generate additional funding for U.S. cyber defense efforts
    - Used to justify efforts to give U.S. government more control over Internet (e.g. control over encryption)

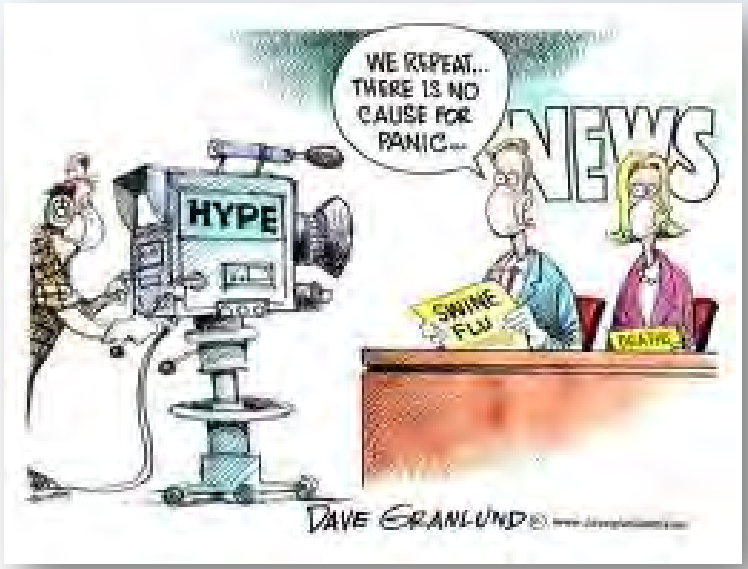
Cyber War is a "Turbo Metaphor"

- Howard Schmidt, recent cyber security coordinator for the White House, supported Schneier's claim by saying, "We really need to define this word because words do matter. Cyber war is a turbo metaphor that does not address the issues we are looking at like cyber espionage, cyber crime, identity theft, credit card fraud [...] Don't make it something that it is not."

Is CyberWar Hype Fuelling a Cybersecurity-industrial Complex?

The Danger of Hype

- Professor Peter Sommer, co-author of a report on cyber war for the OECD, said that "*If you use exaggerated language, you're highly unlikely to come up with good risk analysis and management.*"
- The narrative distorts the public perception of the threats and masks the need for better tools and strategies.



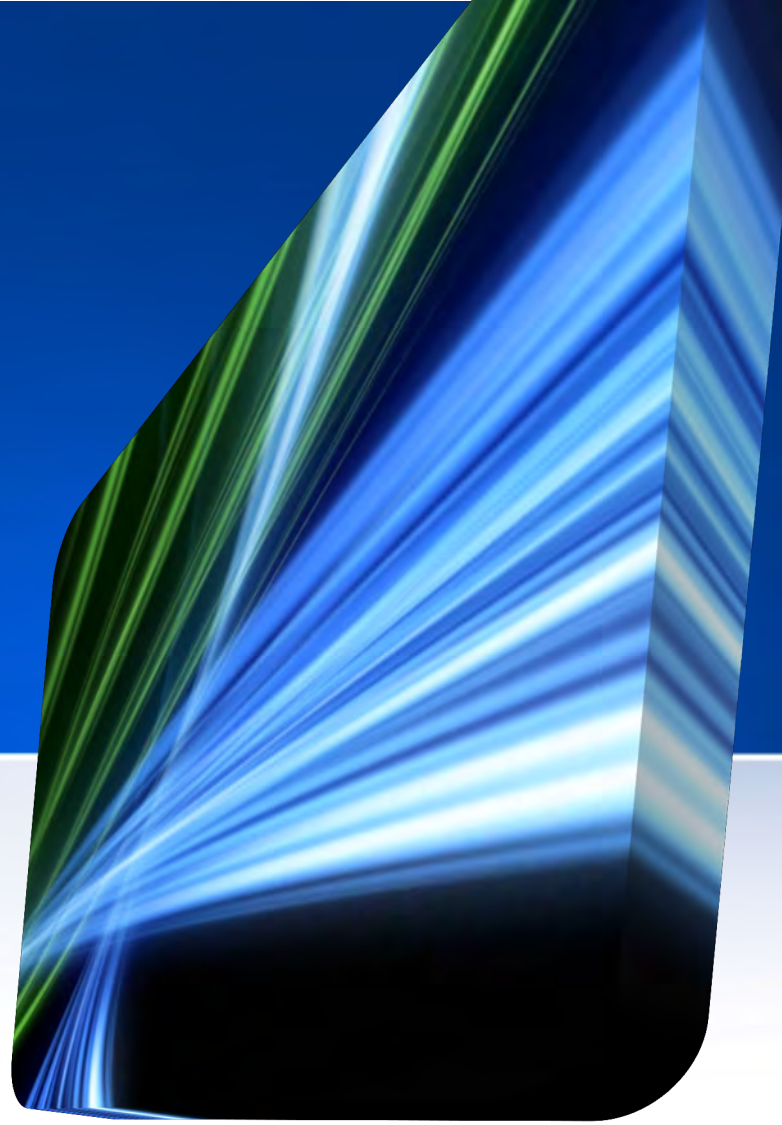
Why Cyber War May Be Unlikely

- Uncertain results such a conflict would bring
- Lack of motivation on the part of the possible combatants
- Shared inability to defend against counterattacks
- Systems that an aggressive cyber attack would damage are valuable to a potential attacker
- Countries capable of large-scale cyber war (e.g., Israel, the U.S., the U.K., Russia and China) have more to lose than they would gain from a cyber attack

Source: McAfee

Internet May NOT a Target for Destruction

- For the Cyber Warrior, Cyber Terrorist, and Cyber Criminal the Internet is a network-mediated communication platform to:
  - Research & Conduct Targeting
  - Conduct Information Operations
  - Collect Intelligence
  - Gain Publicity And Popularity
  - Increase Fundraising
  - Recruit And Train
  - Coordinate Activities
  - Distribute Warnings to Thwart Law Enforcement And Run Counter Intel Operations
  - Spread The Message And Diffuse Propaganda
  - Provide A Platform For Better Communications



FRAMING THE ENVIRONMENT

A Unique Threat

- Unfettered access to cyber weapons systems (i.e., computers and Internet access)
- Immense armies (i.e., botnets that can be captured or rented)
- Capacity for attacks to strike at our nation's most strategic vulnerabilities

Challenges We Face

- IT security arms race - the bad guy is motivated… and patient
  - the adversary able to focus time and money on attacks while the target has to prioritize spending on IT security among other budget items
- Blended Cyber Threats – changing attacks
  - Technology and methods of attack always changing. Can combine several methods of attack

Converging Cyberspace

Cyberterror

Cyberwar

Cybercrime

Does Not Stand Alone

Cyberespionage

The proliferation of capability has enabled a blurring of actors and motivations – a major challenge for cyber security

2007 - Joint Strike Fighter Compromised

- Compromise reported April 2009, started as early as 2007

- $300 Billion project – costliest in US DOD history

- Several Terabytes of data stolen about electronic systems
  - Most sensitive secrets not compromised
- Source of attacks appears to be China

Nov 2008 - Whitehouse email compromised

FT.com FINANCIAL TIMES

In depth

FT Home > In depth > US election 2008

- Front page
- World
- Companies
- Markets
- Markets Data
- Managed funds
- Lex
- Comment
- Video & Audio
- Management
- Business Education
- Personal Finance
- Arts & Leisure
- Wealth
- In depth

US presidential election

Chinese hack into White House network

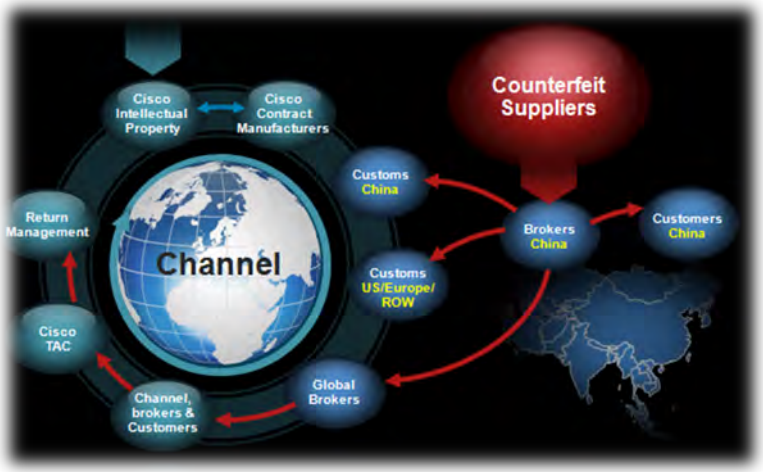
By Demetri Sevastopulo in Washington
Published: November 6 2008 19:13 | Last updated: November 7 2008 00:24

Chinese hackers have penetrated the White House computer network on multiple occasions, and obtained e-mails between government officials, a senior US official told the Financial Times.

On each occasion, the cyber attackers accessed the White House computer system for brief periods, allowing them enough time to steal information before US computer experts patched the system.

2008 – Operation Cisco Raider

- The Feds confiscated more than $75 million of counterfeit Cisco networking gear. The announcement is in a progress report on a two-year-old investigation, code named Operation Cisco Raider. In most cases the fake gear was made in China and imported into the United States where unethical resellers passed it off as legit.
- Intercepted the counterfeit hardware at ports of entry and dismantled illegal supply chains in the US



2008 - Crash of Spanair JK 5022

- Crash of Spanair Flight 5022 at Madrid International Airport on August 20, 2008, killing 154, found that the airline's central computer system used to monitor technical problems in its fleet was infected with malware

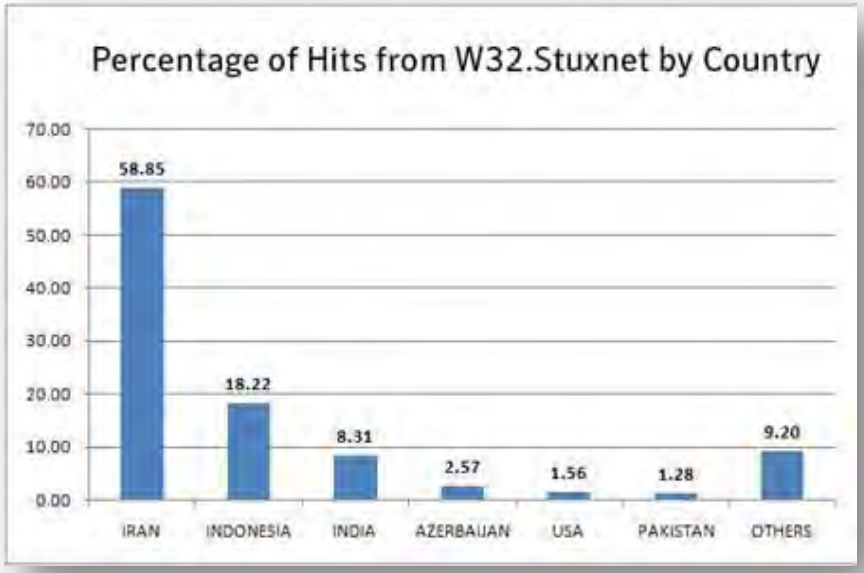
Source: Defense Tech, 20 Aug 10

2008 - Thumb Drive Attack Compromises DoD Computers

- Revealed by DepSecDef William Lynn in Sep/Oct 10 Foreign Affairs Magazine
- A USB flash drive infected with Agent.btz was inserted into a U.S. military laptop at a base in the Middle East
  - "The flash drive's malicious computer code, placed there by a foreign intelligence agency, uploaded itself onto a network run by the U.S. Central Command."
- Spread to classified and unclassified computer systems ; ?? information exfiltrated

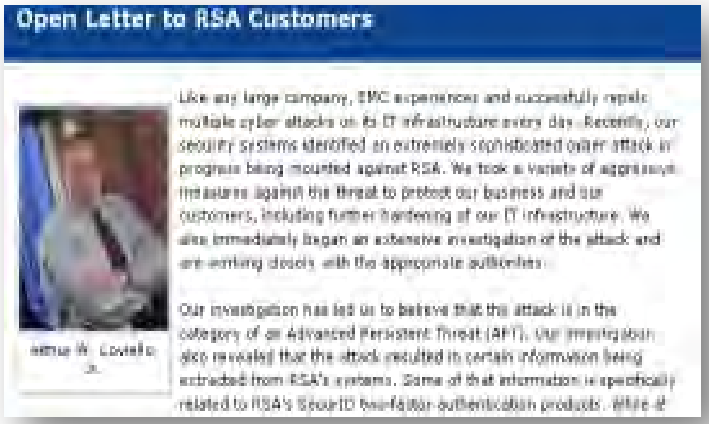
2010 – Stuxnet Malware

- First malicious computer code specifically created to take over systems that control the inner workings of industrial plants
- Actively targeted Windows PCs that managed large-scale industrial-control systems in manufacturing and utility firms
- Iran appeared to be primary target
- Possibly work of state-backed professionals



2011 – RSA Compromise

- Targeted attack that exposed RSA's SecurID technology started with one of the oldest tricks in the book - a phishing email with an infect
- RSA said two different phishing emails were sent to two small groups of low-level users received emails with the subject line "2011 Recruitment Plan" with an Excel attachment that was rigged with the newly patched Adobe Flash zero-day attachment
- The exploit, a Trojan, stole user credentials from RSA employees, including IT staff, and eventually gained privileged access to the targeted system



Source: RSA

2011 - Condé Nast Wires $8 Million to Scammer

- Spear-phishing event
- A scammer created a bank account with a name similar to that of another business that Conde Nast worked with frequently.
- Using the account details in hand, scammer sent an email and requested that all future payments be credited to that bank account.
- Conde Nast signed the “Electronic Payment Authorization” form and faxed it back, essentially giving its bank, JPMorgan Chase, permission to electronically transfer money into that fraudulent account, no questions asked.

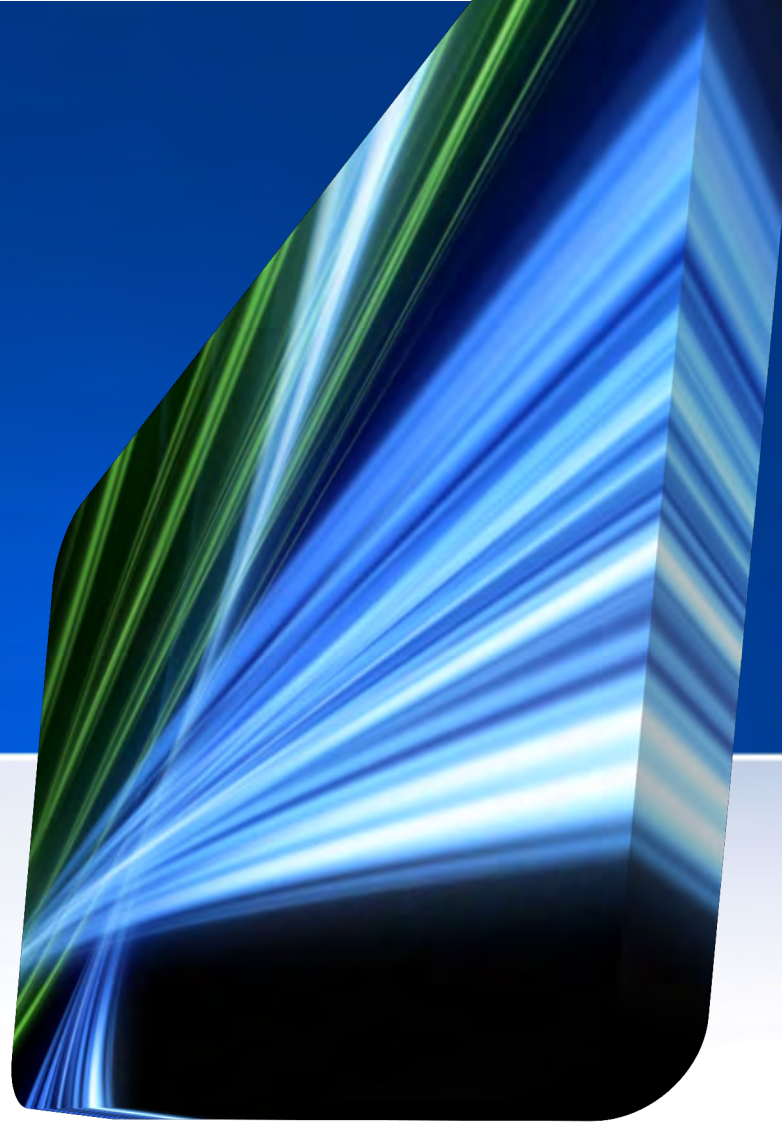
2011 – CIA Hacked by LulzSec

- June 2011 – one of several attacks by Lulz Security on Senate, Sony Corp, and PBS
- LulzSec made claim and published details via Twitter
- Statements made by LulzSec – attacks are a form of protest

2012 – NOAA Hacked by Anonymous

- Various Anonymous sources claimed a hack and defacement against http://www.nwr.noaa.gov/
- Hacker's handle - Codeine

THE PLAYERS



State Actors

- Definition: Nation States who engage in one or more types of cyber operations

Russian Federation	Kyrgyzstan
Ukraine	Estonia
Georgia	Ingushetia
Peoples Republic of China	Taiwan
Israel	Iran
Palestinian National Authority (Hamas)	Myanmar (Burma)
U.S.	Turkey
Pakistan	Germany
Zimbabwe	Australia

Source Jeffrey Carr, GreyLogic

State-Sponsored Actors

- Definition: Non-state actors who are engaged by States to perform one or more types of cyber operations.

Partial list of States known to or suspected of sponsoring Actors
Russian Federation
Peoples Republic of China
Turkey
Iran
United States
Myanmar
Israel

Source Jeffrey Carr, GreyLogic

Non-State Actors

- Definition: Non-state actors who engage in cyber crime and/or patriotic hacking (aka hacktivists)

- Too numerous too list

Let's Look at China

- China may be our number one threat
  - University students on academic visas
  - "Professional" hacking clubs in China
  - Titan Rain intrusion set
- Source code to Microsoft Windows and Office is available in China
- Most of the recent zero-day attacks against Microsoft Office products came from China

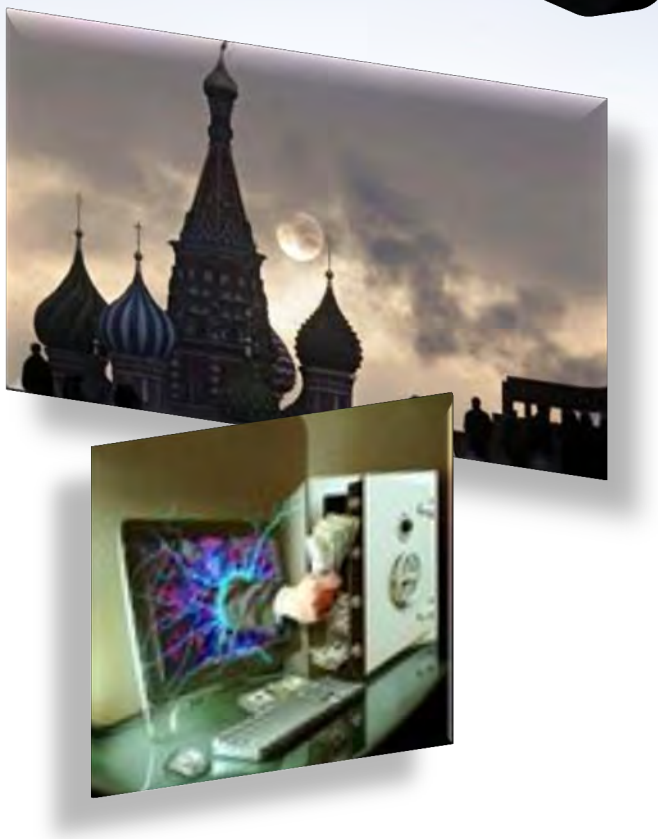
China

- Most skilled vulnerability researchers in the world
- Very capable at command & control networks
- Objective is to steal intellectual property

- Information warfare
  - as a tool of war,
  - as a way to achieve victory without war
  - as a means to enhance stability.
- Strategy
  - “100 Grains of Sand” – infiltrate as many networked systems as possible and lie in wait for sensitive data and/or command and control access.

Is Russia on the Wrong Side of the Net?

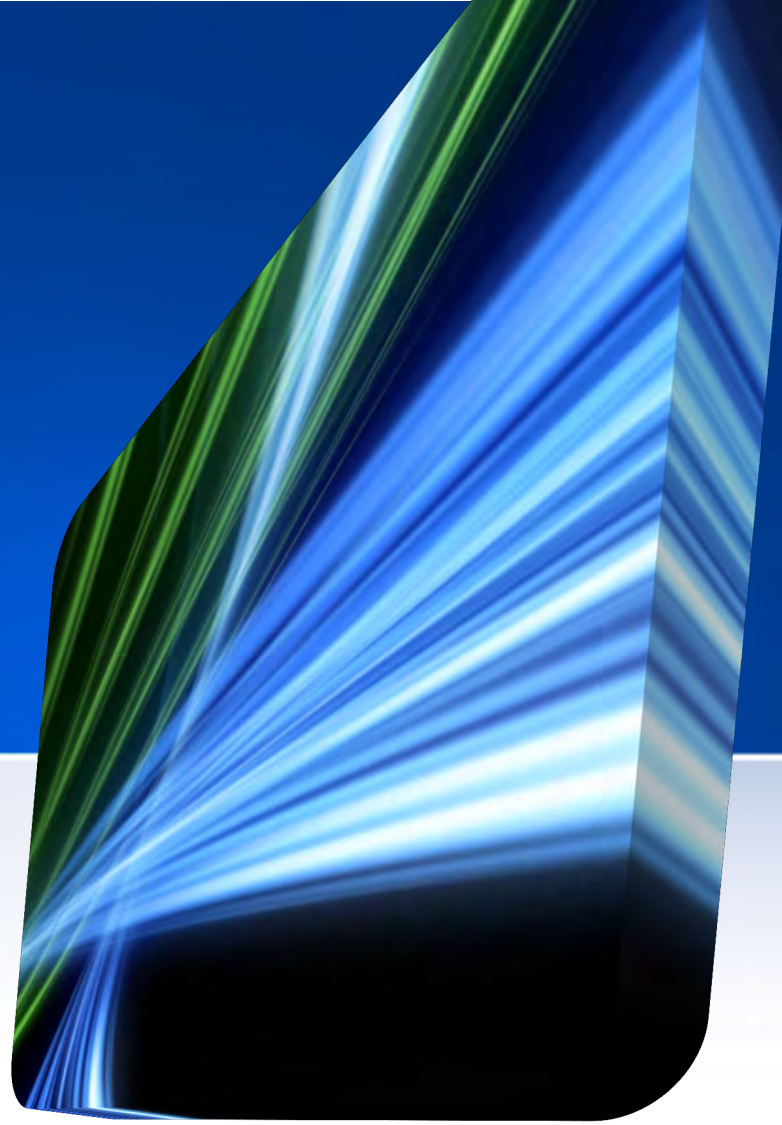
- 2001 European Convention on Cyber Crime
  - Commits signatories to investigate and to co-operate with foreign law enforcement officials dealing with cyber crimes. However, Russia has refused to sign. “This is because the Kremlin’s information warfare actions require plausible deniability, and Russian and CIS hackers and the cyber crime population can provide that,” explained Jeffrey Carr, CEO of Taia Global and author of Inside Cyber Warfare: Mapping the Cyber Underworld.



Is Russia on the Wrong Side of the Net?

- "Russia used to be much more proactive in cracking down on the crime rings that ran the cyber aspect of the criminal business. But Moscow preferred the economic advantage of having such cyber crime groups operate more freely."
  - Iftach Ian Amit, vice president of Security Art, a Tel-Aviv based company
- The criminal Russian Business Network (RBN) "offers a complete infrastructure to achieve malicious activities. It is a cyber criminal service provider."
  - Ramaz Kvatadze, head of the Georgian Research and Educational Networking Association

THE CYBER ARSENAL



Cyber Weapons Proliferation

- The cost to develop cyber weapons is low.
- The raw materials are not restricted and are widely available.
- Weapons can strike at the speed of light, can be launched from anywhere in the world, and can target anywhere in the world.

Cyber Weapons Growth

INTELLIGENCE BRIEFING

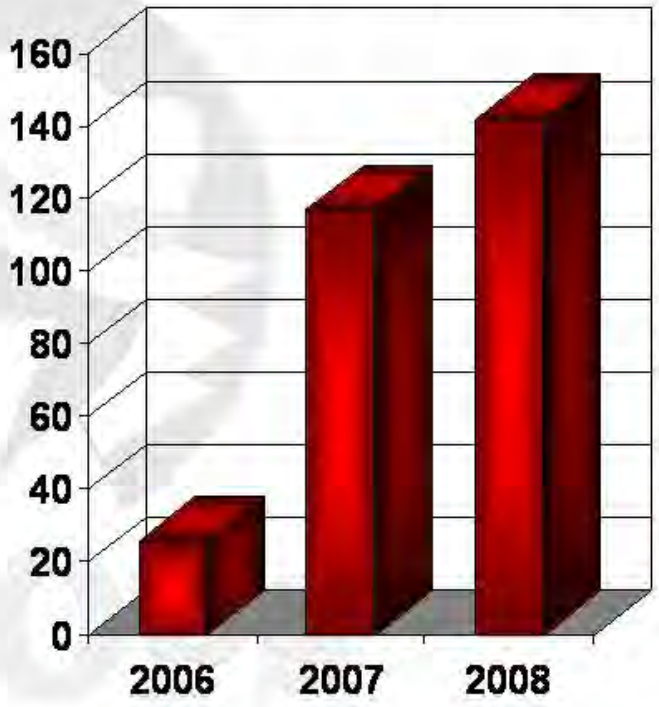
SpyOps

Cyber Weapons Capabilities Growth

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.

Countries with cyber weapons programs



Weapons Economics

What does a stealth bomber cost?

$1.5 to $2 billion

What does a stealth fighter cost?

$80 to $120 million

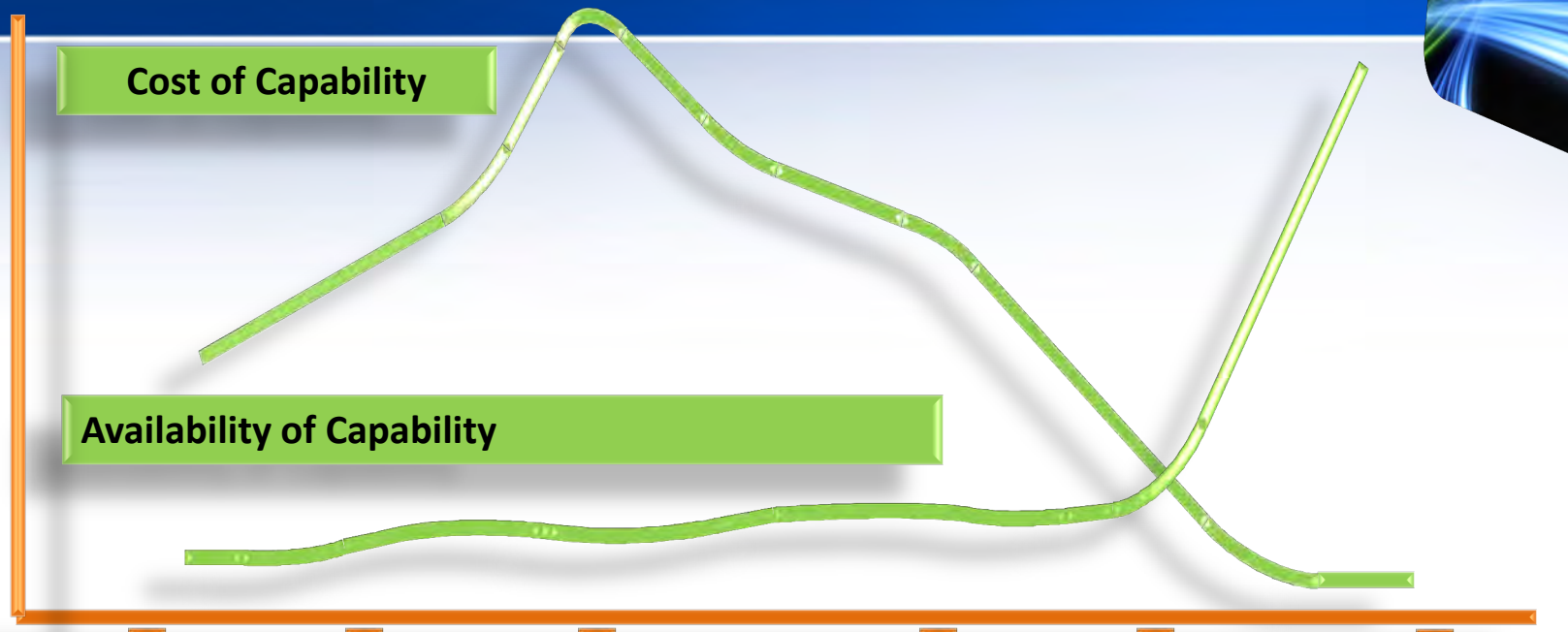
What does an cruise missile cost?

$1 to $2 million

What does a cyber weapon cost?

$300 to $50,000 or less

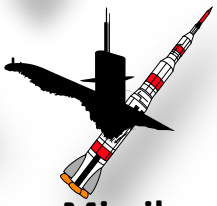
Cost vs. Attack Tools



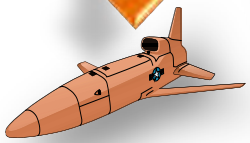
1945 — Infantry

1955 — Strategic Nuclear Weapons

1960 — 1970 — Missiles ICBM & SLBM



1975 — Cruise Missile



1985 — Precision Guided Munitions

Today — Computer

School of Cyber Security LUNARLINE

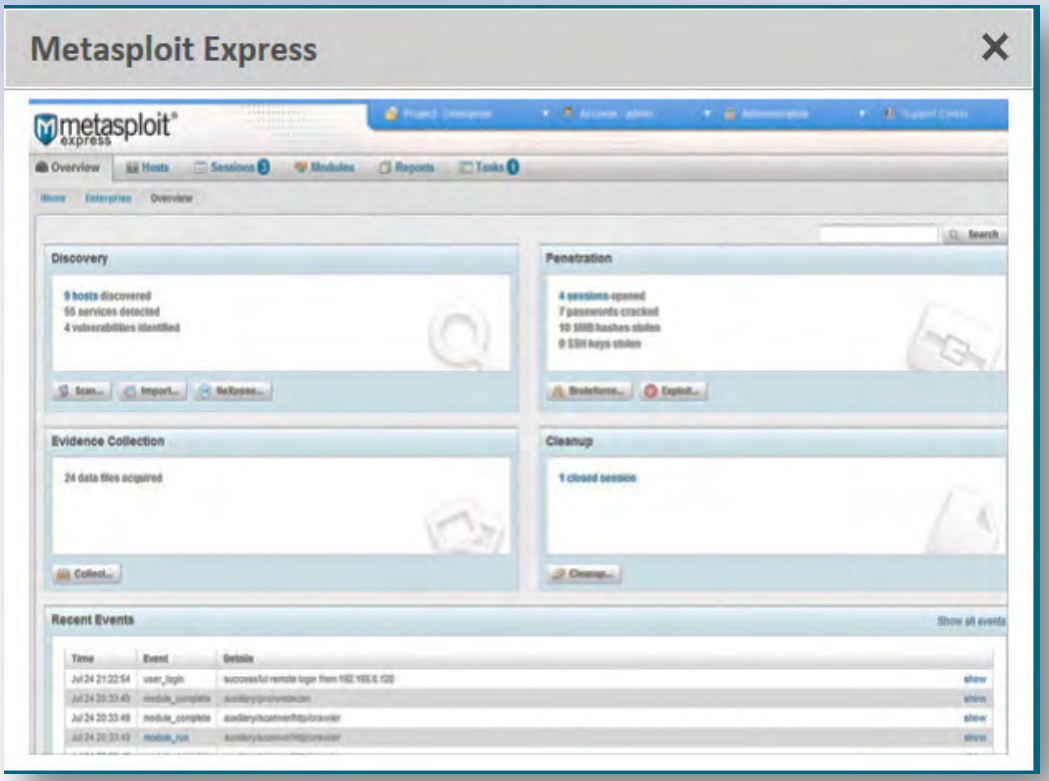
Find the Weapons Facility

Nuclear Weapons Facility

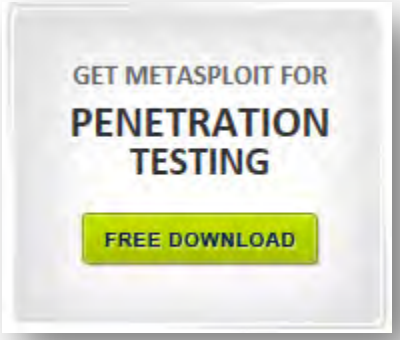
Cyber Weapons Facility

So, where's the Cyber Weapons Facility?

Pure Evil? Metasploit



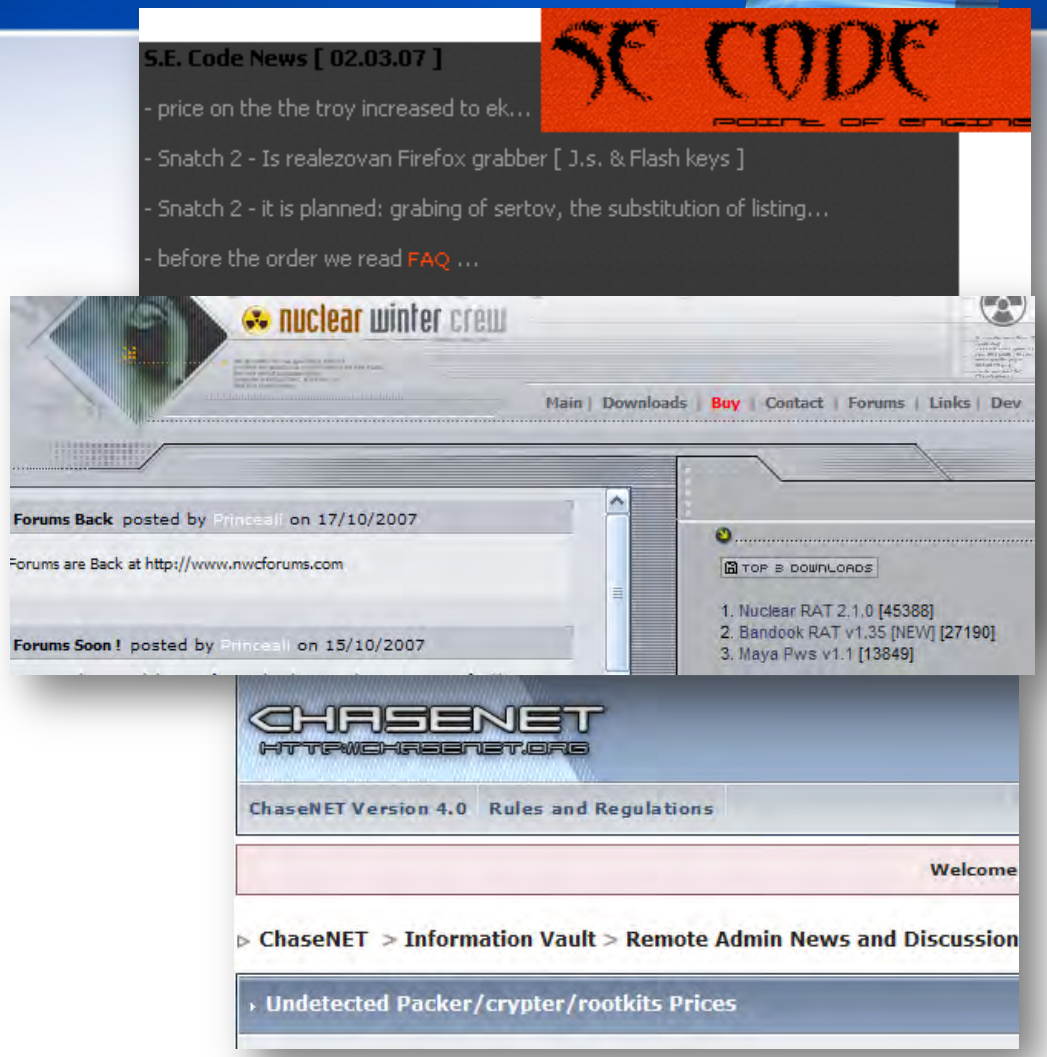
- 3 Versions
  - Community
  - Pro
  - Express



"Metasploit® software helps security and IT professionals identify security issues, verify vulnerability mitigations, and manage expert-driven security assessments." Source: http://www.metasploit.com/

Malware/Phishing Kit – "Arms Suppliers"

- Selling malware for "research only"
- Manuals, translation
- Support / User forums
- Language-specific
- Bargains on mutation engines and packers
- Referrals to hosting companies
- Generally not illegal
- Operate in countries that shield them from civil actions
- Makes it easy to enter the cybercrime market



Proxy Net Providers – “Force Suppliers”

Сетевая безопасность + SEO инструментарий

VPN сервис, Proxy сервис, консалтинг

Мы предоставляем услуги VPN, OpenVPN, а так же прокси сервиса, для Вашей безопасности в сети и работы с поисковыми системами. Также мы занимаемся разработкой и продажей программного обеспечения, для обеспечения Вашей безопасности в сети, системы защиты от DDOS атак, консалтинговые услуги в сфере сетевой безопасности.
В данной сфере мы работаем с 2004 года и имеем огромный опыт оказания подобных услуг.

Описание сервиса, особенности:

уникальные особенности сервиса, аналогов которым не существует где либо еще:

1. ВСЕ прокси в базе проверяются каждые 5 минут ! По этому 99% всех прокси серверов, которые вы увидите в списке - рабочие.
2. Мы даем гарантию на прокси! Если прокси умирает в процессе работы - мы возвращаем вам деньги. Умершие прокси не будут засчитаны.
3. Программа Proxy Helper, с которой вы забудите, что для работы через прокси, нужно копаться в настройках браузера или других программ и постоянно менять там прокси на новые.

Proxy Helper выполняет интеграцию нашего прокси сервиса и ваших программ, вы просто выбираете нужный прокси и сразу, без захода в какие либо настройки, работаете через него. Аналогов не существует.

Так же внутри вас ждет множество приятных мелочей, при наличии которых работать становится удобнее и приятнее. AnyProxy.net - сервис, который приятно удивит вас.

Все прокси в списке - SOCKS 4/5, так же есть возможность использовать анонимные HTTP/HTTPS/FTP прокси*, время жизни одного отдельно взятого прокси сервера составляет максимум 24 часа.

Все прокси сервера отсортированы по городам, странам, штатам (для США), типу подключения к сети, скорости, времени онлайн, домену, также есть поиск по всей базе по любому параметру.

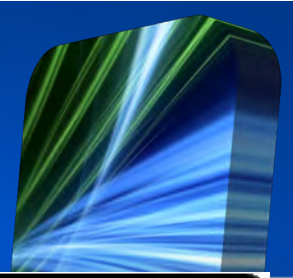
Если вам чтото не подошло, moneyback гарантирован в течении 2х дней со дня начала пользования сервисом, за вычетом стоимости 2х дней.

* - при использовании Proxy Helper

Тарифы

Daily plans ***						Per Use plans				
цена 1 прокси	дневной лимит **	**цена (в месяц)**	название тарифа	**кол-во в месяц***	**Proxy Helper**	цена 1 прокси	**цена (в месяц)**	название тарифа	**кол-во в месяц***	**Proxy Helper**
0.13¢	5	**$25**	Daily 5	**150**	$10	0.50¢	**$9.95**	PerUse 1	**20**	$10
0.11¢	10	**$40**	Daily 10	**300**	$10	0.30¢	**$15**	PerUse 2	**50**	$10
0.08¢	20	**$50**	Daily 20	**600**	$10	0.25¢	**$20**	PerUse 3	**80**	$10
0.07¢	30	**$65**	Daily 30	**900**	**free !**	0.15¢	**$29.95**	PerUse 4	**200**	$10

Buy an Exploit – "Intelligence Dealers"



MarketPlace | About | Services | FAQ | Blog | Careers | Contacts

WabiSabiLabi
CLOSER TO ZERØ RISK

Home page ▸ Current bids

Sign in

Username
Password
Sign in

New user? Sign up here

News

WSLabi Reports... 18/10/2007
darkreading.com

Capitalising on... 18/10/2007
computerweekly.com

"Ebay" für Software... 18/10/2007
computer-zeitung.de

See all news

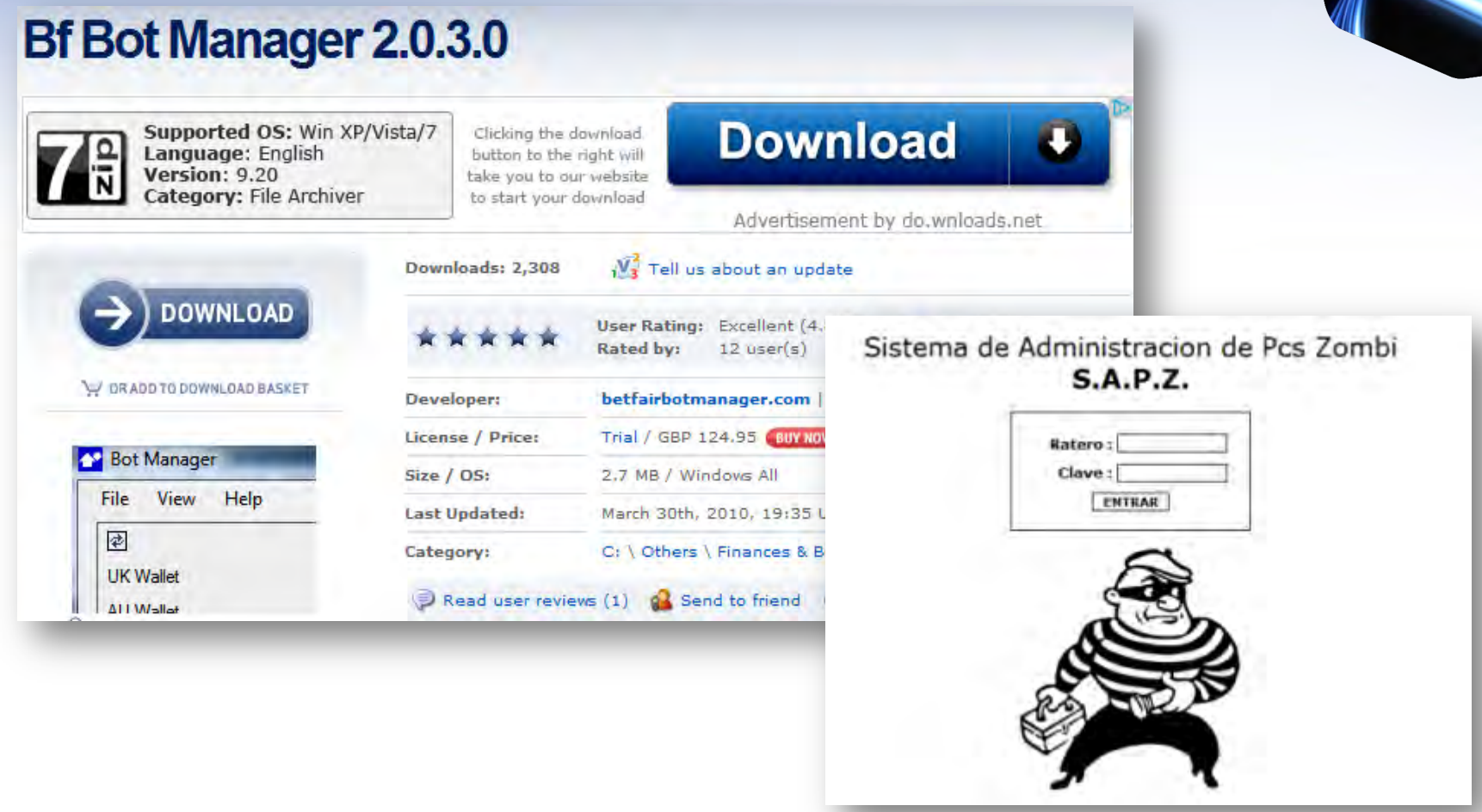
Current bids | MarketPlace history

16 items found, displaying all items.

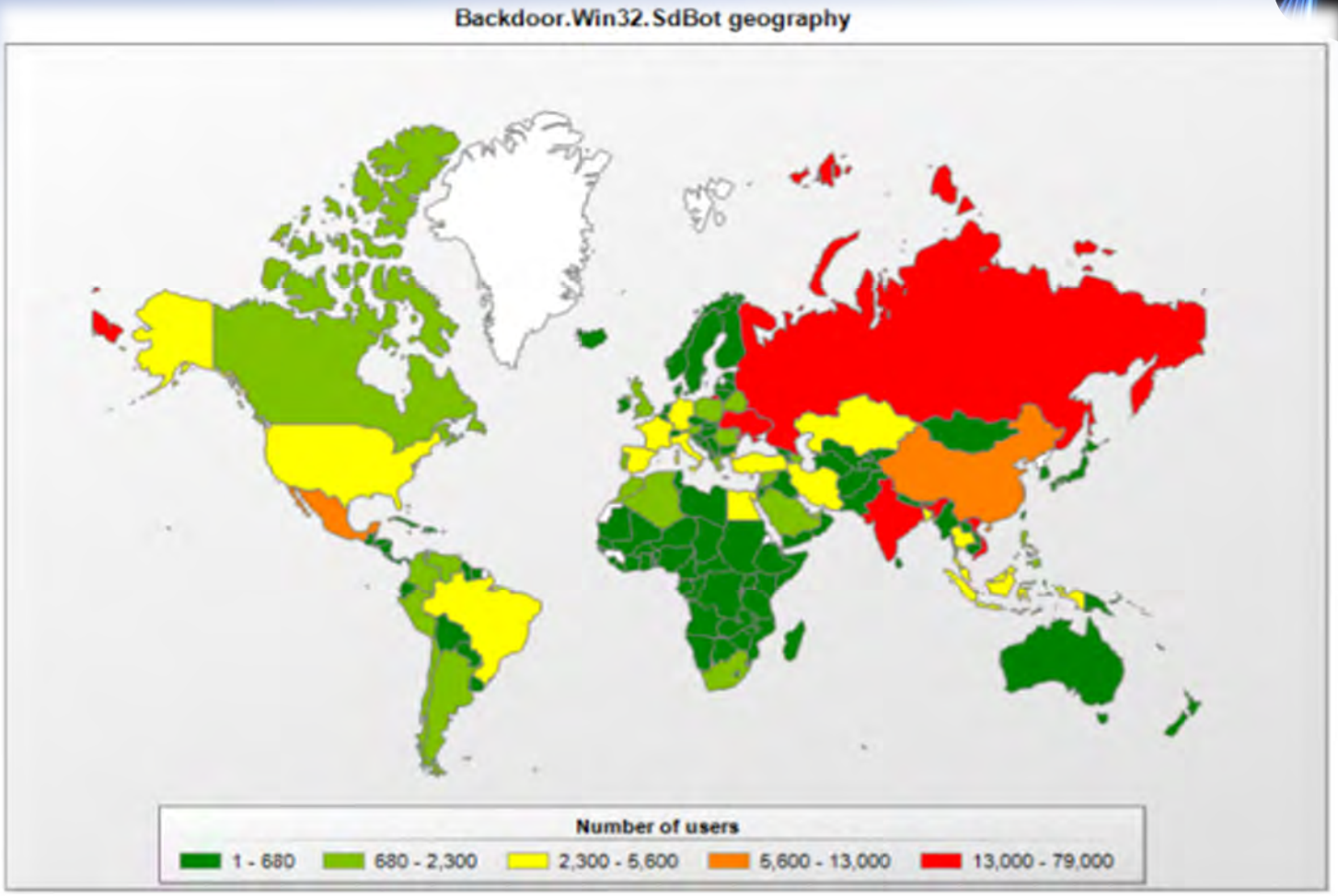
Page 1

Code	Time to live	Title	System	Offer type	Last bid	
ZD-00000152	0d 15h 17m	SAP MaxDB	Linux	Auction Buy now at Buy exclusively at	0€ 0 bid(s) 15,000€ 30,000€	info
ZD-00000146	0d 15h 17m	VanDyke VShell	Windows 2000	Auction Buy now at	0€ 0 bid(s) 500€	info
ZD-00000134	0d 15h 17m	Novell	Windows XP	Auction Buy now at	0€ 0 bid(s) 5,000€	info
ZD-00000133	0d 15h 17m	IBM	Windows XP	Auction Buy now at	0€ 0 bid(s) 5,000€	info
ZD-00000130	1d 15h 17m	Microworld eScan Anti-Virus	Linux	Auction	0€ 0 bid(s)	info
ZD-00000144	12d 15h 17m	FreeRadius	Linux	Auction	0€ 0 bid(s)	info
ZD-00000138	12d 15h 17m	Novell GroupWise	Web application	Auction	1,000€ 1 bid(s)	info
ZD-00000132	12d 15h 17m	Novell eDirectory	Linux	Auction	0€ 0 bid(s)	info
ZD-00000131	12d 15h 17m	Samba	FreeBSD	Auction	0€ 0 bid(s)	info
ZD-00000114	12d 15h 17m	PHPMyAdmin	Web application	Auction	0€ 0 bid(s)	info
ZD-00000072	12d 15h 17m	DWebPro	Windows Server 2003	Auction	0€ 0 bid(s)	info
ZD-00000069	12d 15h 17m	ClamAV	Linux	Auction	0€ 0 bid(s)	info
ZD-00000065	12d 15h 17m	Weird Solutions BOOTPTurbo	Windows XP	Auction Buy exclusively at	0€ 0 bid(s) 500€	info
ZD-00000045	12d 15h 17m	myBloggie #2	Web application	Auction	0€ 0 bid(s)	info
ZD-00000145	13d 15h 17m	RealNetworks Helix Server	Linux	Auction	0€ 0 bid(s)	info
ZD-00000017	13d 15h 17m	MailEnable	Windows 2000	Auction	0€ 0 bid(s)	info

Bot Management– "Turn Key Weapons Systems"



Botnet Geography



Source: Kaspersky Labs

Cybercrime - Ammunition

Zeus Builder – God of Do-It-Yourself Botnets

ZeuS Builder

Information
Builder

Builder
Config and loader building
Source config file:
D:\temp

Output
Loading
Loading
Building
botnet=
timer_co
timer_lo
timer_st
url_conf
url_comp
encrypti
blacklist_
Build suc

View report (HTTP request, 172 bytes)

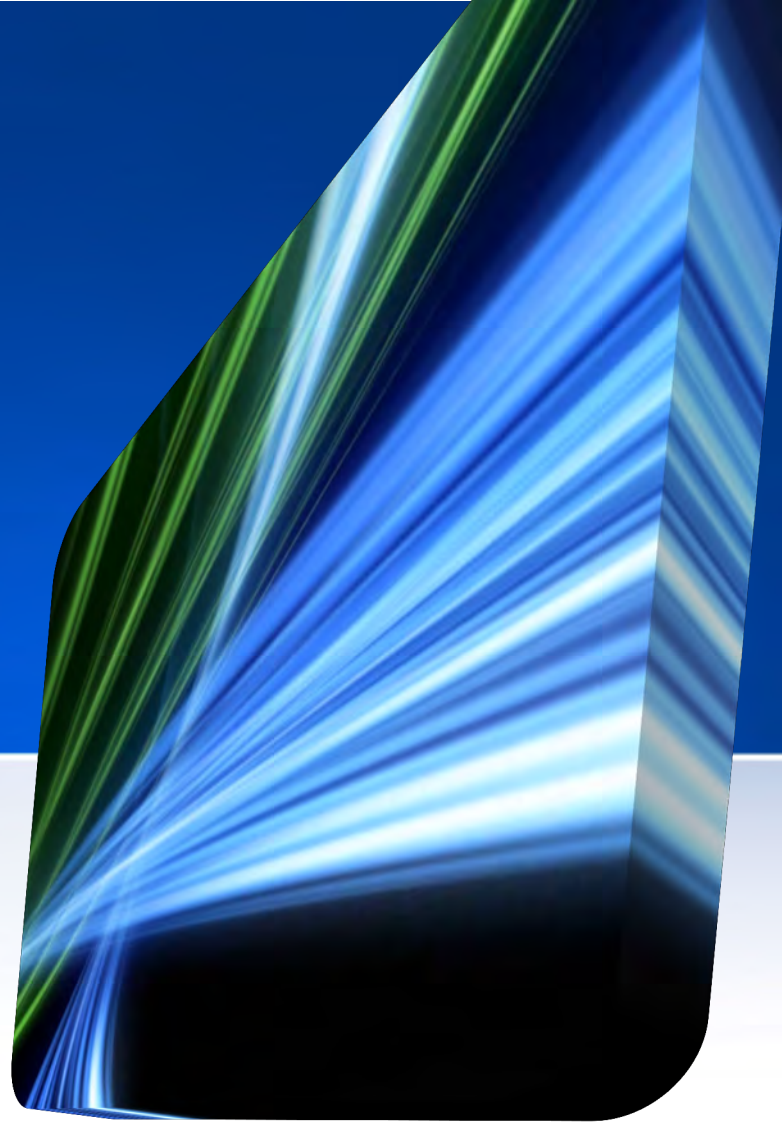
Bot ID:	**bot_10000001**
Botnet:	plag
Version:	1.2.4.2
OS Version:	XP Professional SP 2, build 2600
OS Language:	1033
Local time:	30.09.2009 14:16:03
GMT:	-8:00
Session time:	04:35:50
Report time:	30.09.2009 21:15:41
Country:	--
IPv4:	192.168.1.83
Comments for bot:	-
In the list of used:	No
Process name:	C:\Program Files\Internet Explorer\iexplore.exe
Source:	http://www. bank.com/login.php

```
http://www. bank.com/login.php
Referer: http://www. bank.com/login.html
Keys: admintestswordfish1234567890
Data:

username=admintest
password=swordfish
pinnumber=1234567890
```

Password Capture Report

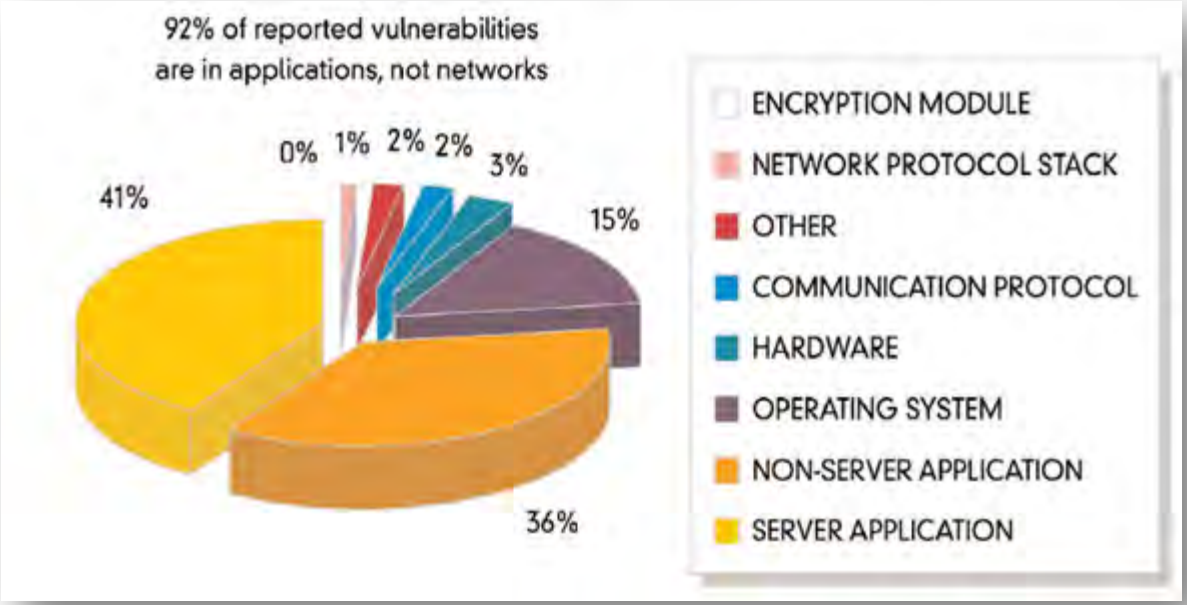
RELATED AREAS OF CONCERN



Some Noted Cyber Security Menaces

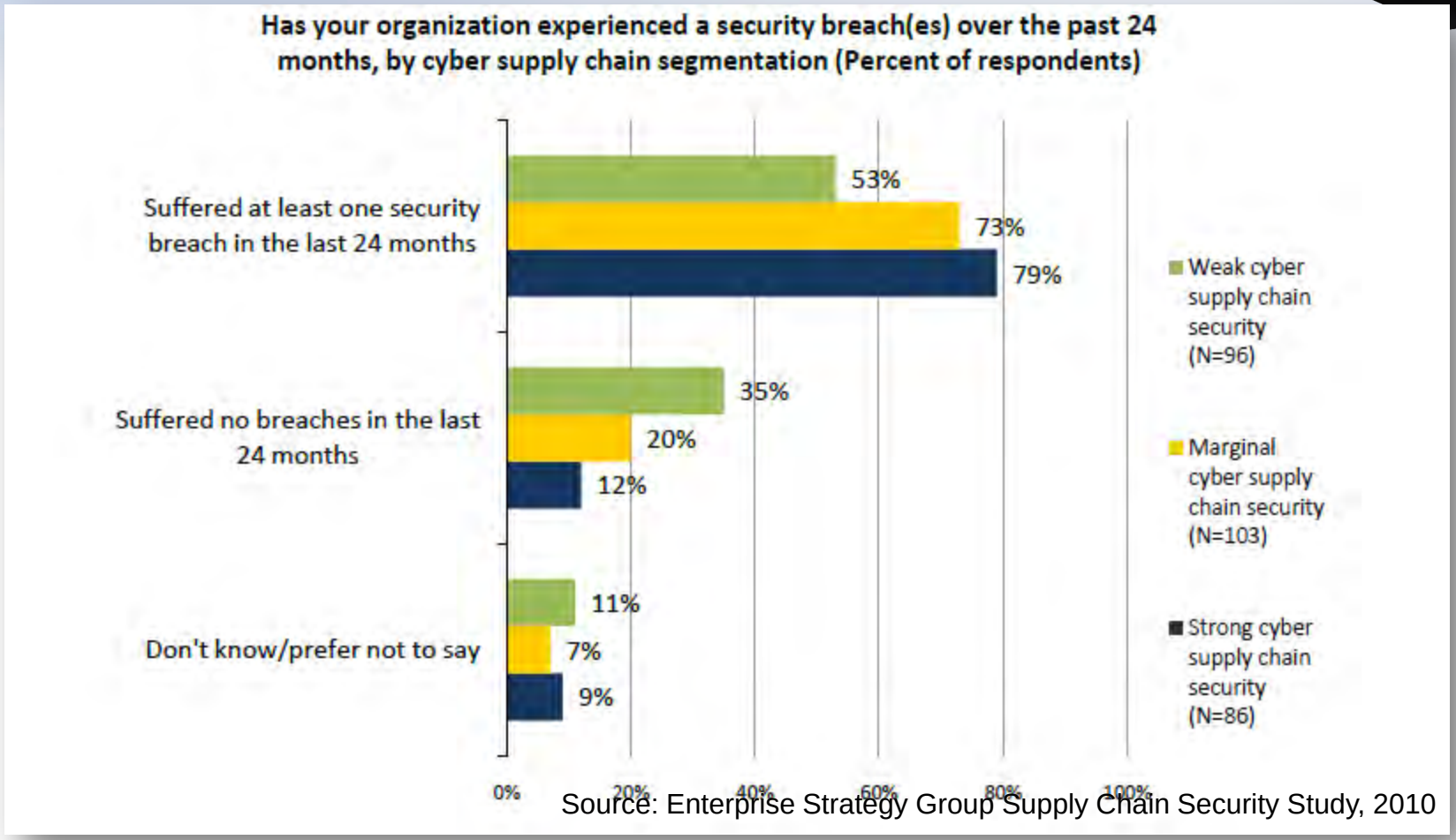
System & Software Assurance

- “What is also surprising is that we, private citizens and governments alike, tolerate these technical vulnerabilities and their consequences as the price to pay for innovation and competition in a free market. Today, we would not tolerate a car built and then driven on our networks of roads without brakes or with a feeble braking system. Why then do we accept insufficient safety measures on the information highway?” Dr. Audrey Guinchard, Senior Lecturer in Law, University of Sussex



Supply Chain Vulnerability?

Based on a study involving 285 critical infrastructure companies:

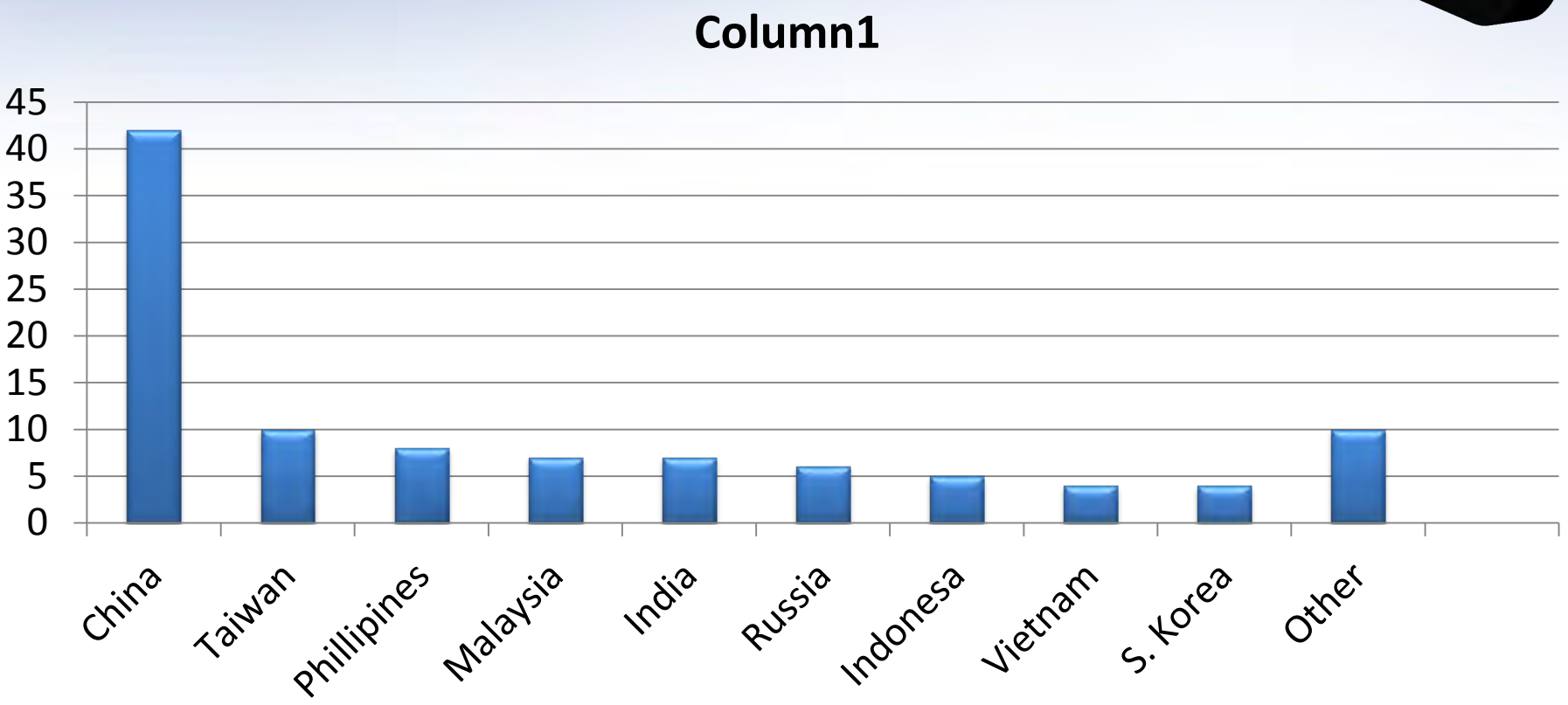


Source: Enterprise Strategy Group Supply Chain Security Study, 2010

How Do We Buy Stuff?

- Directly from Source (PRC???)
- Through Another Country (Canada???)
- Contractors and Sub-Contractors
- Government Credit Card
- e-Bay (!!!)

Top Countries Suspected/Confirmed to be Sources of Counterfeits*



Source: U.S. Department of Commerce, Office of Technology Evaluation, *Counterfeit Electronics Survey*

Wikileaks – Is It Really Cyberwar?

- "*The first serious info war is now engaged. The field of battle is WikiLeaks*," Electronic Frontier Foundation co-founder John Perry Barlow tweeted Friday, 3 Dec.
- Cyberterror? Cyberhacktivism?

Wikileaks

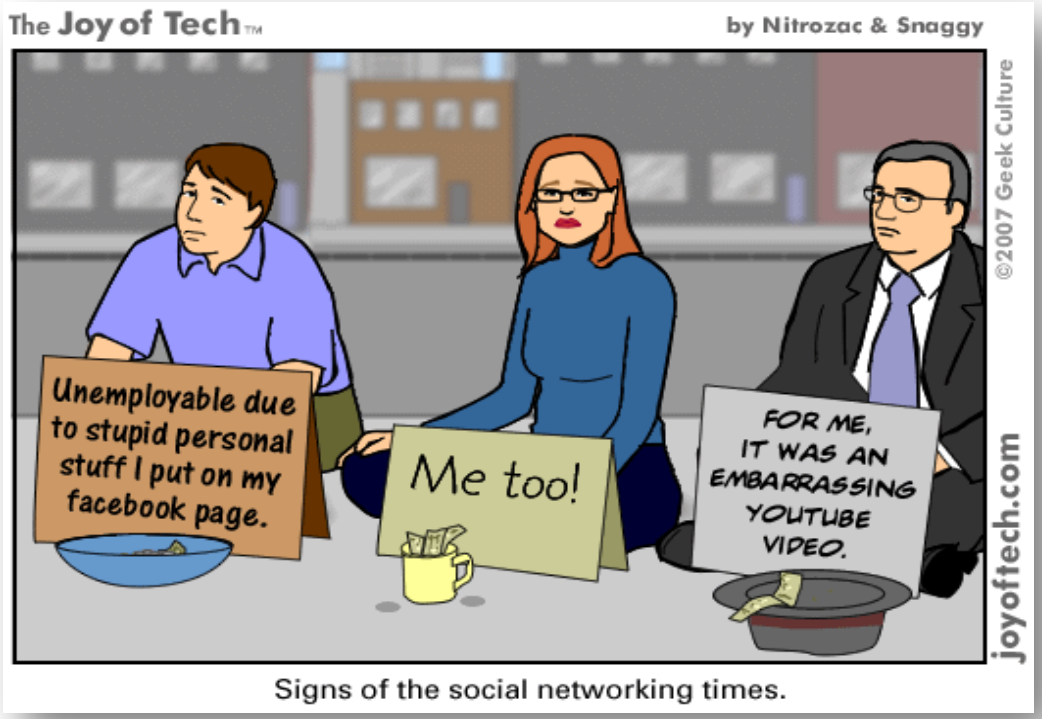

We all only live once. So we are obligated to make good use of the time that we have and to do something that is meaningful and satisfying. This is something that I find meaningful and satisfying. That is my temperament. I enjoy creating systems on a grand scale, and I enjoy helping people who are vulnerable.
And I enjoy crushing bastards.
- Julian Assange

Exfiltration

Source: Strotz Friedberg

Social Media - Security Risks?

Can result in social engineering, identity theft, financial fraud, infected computers, stalking, child abuse, sexual predation, defamation, lawsuits, mad boyfriend/girlfriend/spouse/parent, unwanted legacy, embarrassment, …



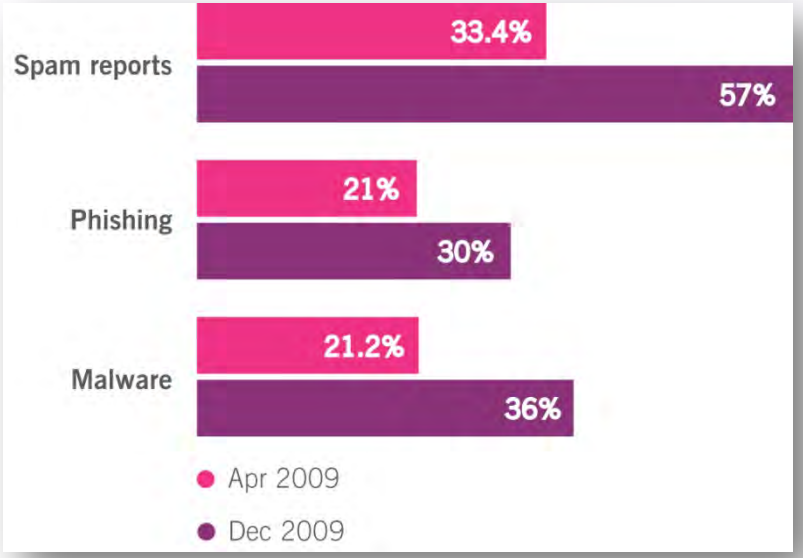
Signs of the social networking times.

Social Media Attacks On The Rise

- Spam, phishing and malware attacks through social media are growing:

- 70% rise in firms encountering spam and malware attacks via social networks in 2009
  - Over 50% received spam via social networks
  - Over 33% received malware via social networks

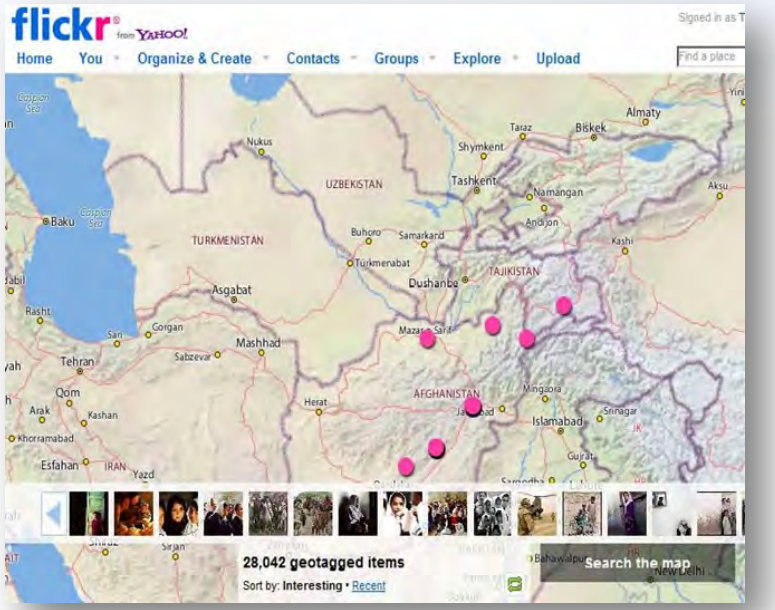
Organizations that have been victims of attack through social networking sites



Source: Sophos survey 2010

Do We Reveal Too Much?

- Main function of location-based social networking applications is to broadcast a user's specific location
  - Collect points, badges, or other rewards
- Simple search for Afghanistan on flickr revealed at least 28000 geo-tagged items



Evolution of Mobile Malware

Criminals now using PC-style malware attacks to infect mobile devices

Greatest mobile malware risk comes from rapid proliferation of applications in app stores

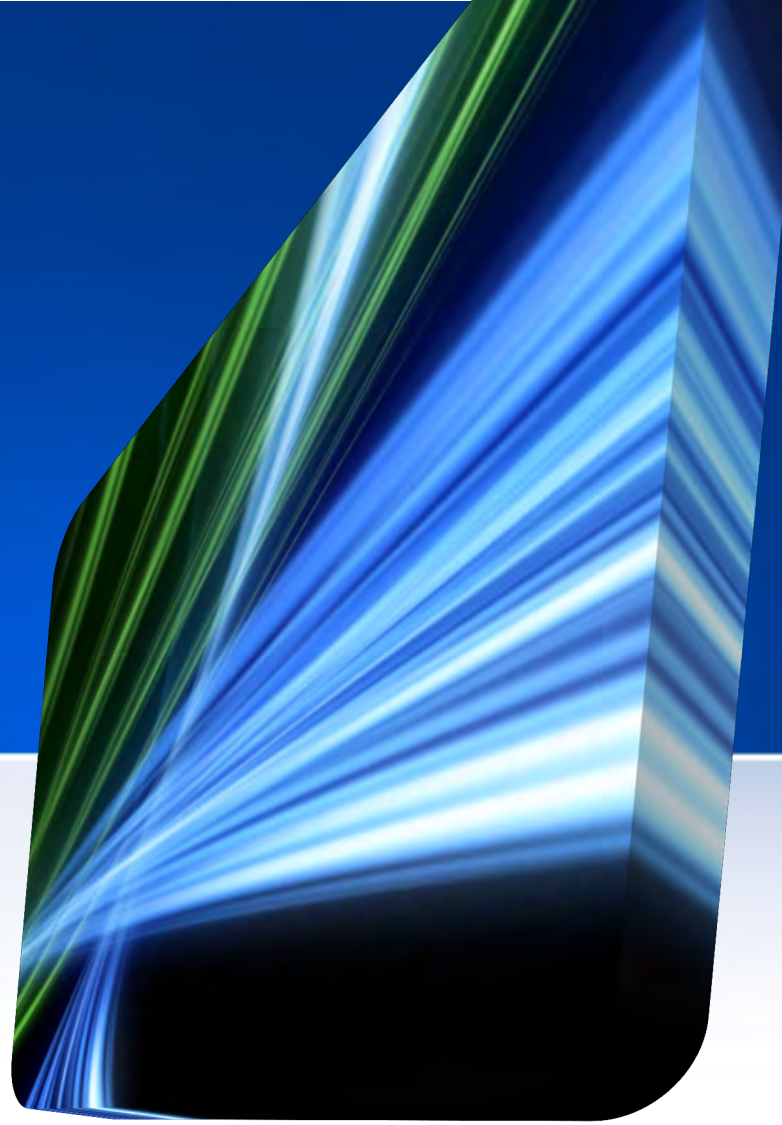
Mobile spyware is prevalent and now commercialized

2009 → 2010

Between 2009 and 2010, reported increase in mobile threats of 250%*

Information obtained from analysis of Juno's Pulse Mobile Security Suite virus definition database dated 10/15/2010

A PLAN FOR ACTION



The More Things Change, The More They Stay the Same

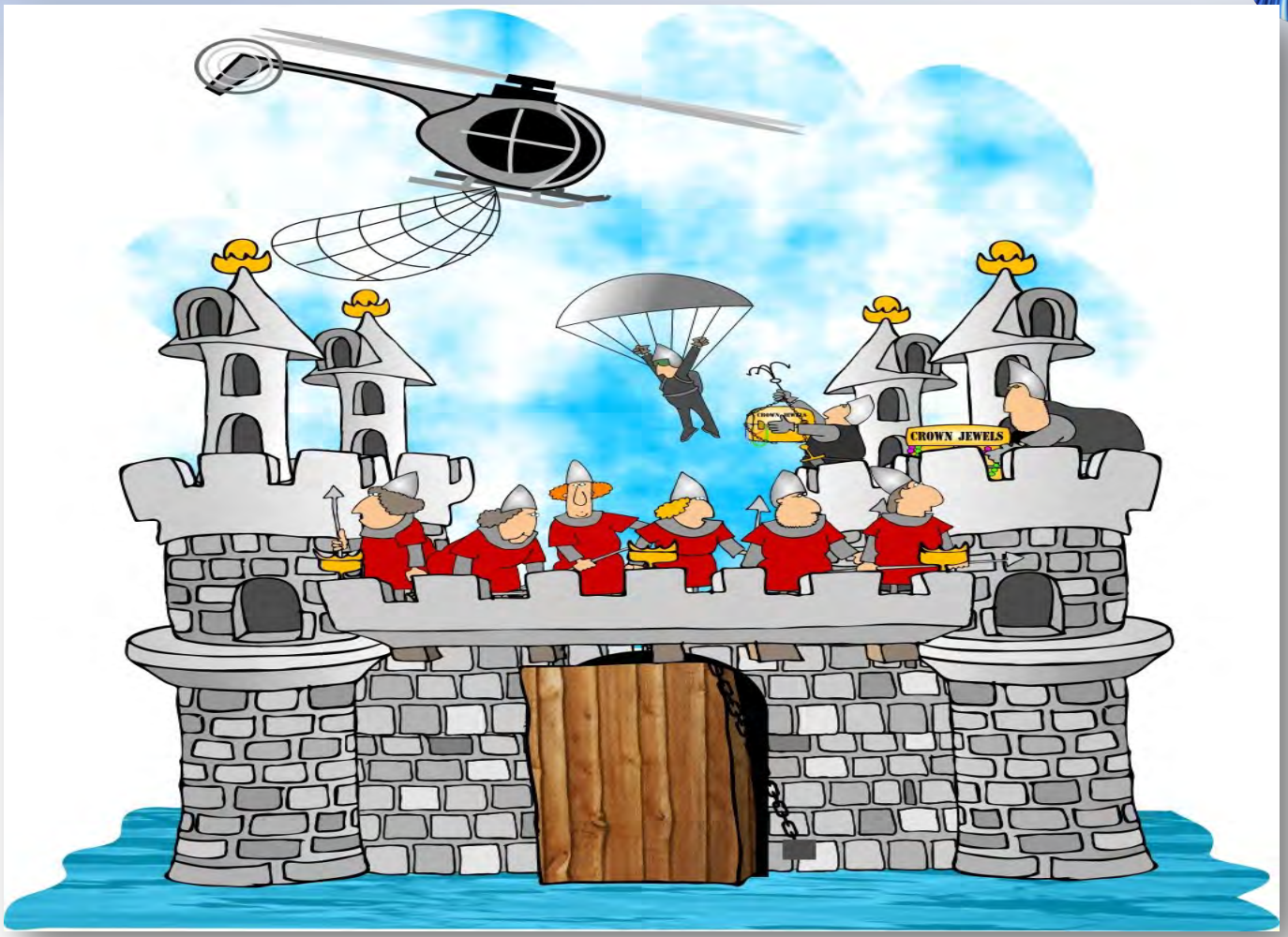
- "Wars in the 21st century will increasingly require all elements of national power – not just the military. They will require that economic, diplomatic, financial, law enforcement and intelligence capabilities work together."

Former Secretary Rumsfeld address to the National Defense University, January 31, 2002.

US Difficulties in Mounting a Cyber Defense

- Internet created in USA in an environment of intellectual freedom, mostly under private (not government) control
  - Efforts to change – e.g. “Kill Switch” bill (2010) in Congress giving government power to take over parts of internet in national emergency
  - Other countries can more easily mount defense (e.g. fewer entry points, government can already control networks)
- US military cyber-capabilities are significantly focused on offense, not defense

Traditional Countermeasures Can Fail!



What Should You Do?

We Need A Cohesive Strategy

Mike McConnell, former DNI, stated:

"The United States is fighting a cyber-war today, and we are losing. It's that simple. The problem is not one of resources; even in our current fiscal straits, we can afford to upgrade our defenses. The problem is that we lack a **cohesive strategy** to meet this challenge."

Suggestions for Action

- Suggestions:
  - 1) Enact limited government regulation of internet, cyberspace
    - Need international cooperation as well as national efforts
  - 2) Increase resources for cyber-defense (government, private)
  - 3) Isolate critical infrastructure (e.g. power grid) from the internet
    - Source: Richard A. Clarke, “Cyber War”
  - 4) Investigate cyber-treaties

Additional Options for Action

- Deploy information systems developed to not just be functional but secure
  - Bolting on security or patching vulnerabilities is just the digital equivalent of the Maginot line
- Establish a more secure and resilient digital infrastructure
- Protect the information – not only the shell that houses it
- Insist on a secure supply chain
- Improve application level security and software assurance
- Make security transparent as possible – if security is inefficient, inconvenient, and inflexible in time of crisis if will guarantee that users will seek ways around the rules

Moderating Effects to 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

A Necessary Paradigm Change

- Stop being defeatist.
  - Don’t accept a state of insecurity and technological inadequacy.
- Work an attitude change in the private sector.
  - Government must partner with the private sector and hold the critical private sector systems accountable.
- Change the attitude of the general public.
  - Create an understanding that there may need to be an exchange of convenience for security.

Time for Discussion

References

- Claburn, Thomas. Operation Cisco Raider Nets $76M in Fake Gear. Information Week, February 2008
- Fallier, Nicolas; O Murchu, Liam; and Chien, Eric. W32 Stuxnet Dossier. Symantec, November 2010
- Gorman, Siobhan; Cole, August; and Dreazen, Yochi. Computer Spies Breach Fighter Jet Project. The Wall Street Journal, April 2009
- Habinger, Eugene. Cyberwarfare And Cyberterrorism: The Need For A New U.S. Strategic Approach. CSI, February 2010
- Lynn, William. Defending a New Domain. Foreign Affairs, September/October 2010
- McConnell, Mike. How to Win the Cyberwar We're Losing. The Washington Post, February 2010
- Meyer, David. Report: Trojan a factor in fatal Spanair crash? Cnet News, August 2010

References

- War in the Fifth Domain. The Economist, July 2010
- Enterprise Strategy Group Research Report. Assessing Cyber Supply Chain Security Vulnerabilities Within the U.S. Critical Infrastructure, Nov 10
- Kapsersky Reports. IT Security for the Next Generation, 2010
- US Department of Commerce. Defense Industrial Base Assessment: Counterfeit Electronics, Jan 10
- Homeland Security Newswire. Defining cyber warfare, Feb 11
- Russia Today (RT) Network. Is cyberwar hype fuelling a cybersecurity-industrial complex? , Feb 12