

# Cyber War, Cyber Terrorism and Cyber Espionage (v1.2)

Joe St Sauver, Ph.D.  
(joe@uoregon.edu or joe@internet2.edu)  
Security Programs Manager, Internet2

IT Security Conference  
Fargo, ND  
October 21-22, 2008

<http://www.uoregon.edu/~joe/cyberwar/>

**Disclaimer:** All opinions expressed are solely those of the author and do not necessarily represent the opinions of any other entity.

# **I. Introduction**

# Disclaimers

- I'm **not** a cyber defense guy **nor** am I a cyber intelligence person, so some of you may wonder, "Hey, why should I trust what Joe tells me?" My answer would be "Please DON'T! Think carefully about what I say and verify it yourself!"
- Since today's topic is quite a sensitive one, I've made a conscious effort to be very careful about what I say since I have no desire to help the bad guys. I've thus restricted myself to material that is unequivocally public, often material published in the news media.
- At the same time, cyber war, cyber terrorism, and cyber espionage are topics of increasing timeliness, and our nation and its citizens will be ill prepared to deal with these threats if those topics never get any discussion whatsoever. Hence, today's talk.
- I'd also like to take thank those who offered comments on a draft of today's talk, including Jose Nazario, Ph.D., of Arbor Networks, and Steven Bellovin, Ph.D., of Columbia University. Despite that feedback, all opinions expressed in this talk are solely my own responsibility and do not necessarily represent any other entity<sub>3</sub>

# Format of This Talk

- This talk has been prepared in my normal unusually-detailed format. I use that format for a number of reasons, including:
  - doing so helps to keep me on track when I have limited time
  - audience members don't need to scramble to try to take notes
  - if there are hearing impaired members of the audience, or non-native-English speakers present, a text copy of the talk may facilitate their access to this material
  - a detailed copy of the talk makes it easy for those who are not here today to go over this talk later on
  - detailed textual slides work better for search engines than terse, highly graphical slides
  - hardcopy reduces problems with potential mis-quotation
- BUT I promise that won't read my slides to you, and I also promise that I won't go over my time. Speaking of time...

# We Don't Have Time To Talk About Cyber Crime

- While cyber crime is a very serious problem, with only 55 minutes for this presentation, there's simply no time to talk about cyber crime AND cyber war AND cyber terrorism AND cyber espionage during today's time slot.
- If you're interested in my "take" on cyber crime, please see:  
"A Succinct Cyber Crime Tour Meant To Illustrate By Way of Assorted Examples The Sort of Online Crimes Which Are Occurring -- And Why We Need More Cyber Crime-Trained Attorneys," <http://www.uoregon.edu/~joe/tour/cybercrime.pdf> from January 8th, 2008 (122 slides)
- Think of this talk as the companion piece or "complement" to that earlier talk, addressing the areas it had intentionally excluded.

# Why Talk About Cyber War, Cyber Terrorism and Cyber Espionage HERE, in North Dakota?!?

- Some folks might assume that “ground zero” for any cyber war would be Washington DC, as the seat of government, or perhaps our largest cities -- New York, Chicago, San Francisco, L.A., etc.
- At least in some scenarios, however, it is North Dakota which is squarely in the cross hairs. Why? Well, among other things, North Dakota plays a key role in our nation’s defense, hosting critical elements of our national nuclear deterrent forces.
- For example, just thinking about ICBMs, **North Dakota is home to the 91st Missile Wing at Minot Air Force Base, one of only three remaining ICBM bases in the United States** (the other two being the 90th Missile Wing at Warren Air Force Base, Wyoming, and the 341st Missile Wing at Malmstrom Air Force Base, Montana). I bet that our enemies have a high level of interest in all three of those sites...

## **“But That’s the Air Force, Not Us!”**

- The military world and the civilian world overlap and intertwine, and there’s no sharp bright line cleanly separating the two.
- One implication of this becomes clear when we think about our enemies attacking a military base by targeting base personnel.
- NCOs, officers, and civilian base employees will often:
  - have off-base housing with community-provided utilities (such as home telephone service and home Internet service), or they
  - may have bank accounts with local banks or credit unions, etc.
- Do you think there’s any chance that the bad guys might try to “get at” those personnel via those community contacts?
- For example, maybe our enemies would try dropping malware on customers of local ISPs, hoping that one of those customers might be a base employee working at home on confidential documents, or phishing local banks to look for base personnel with financial difficulties... In fact...

# How About Non-Military Critical Infrastructure in North Dakota?

- **Is there commercial critical infrastructure in ND? \*YES\***
- **Key pipelines:** Alliance Pipeline, Enbridge Crude Oil Pipeline, Kaneb Product Pipeline, Northern Border Pipeline System (see the downloadable maps at [www.rentagstrategies.com/downloads](http://www.rentagstrategies.com/downloads) )
- **Electrical transmission infrastructure:** Check out the area coincidentally selected for “transmission infrastructure” at [www.globalenergymaps.com/electric-map.html](http://www.globalenergymaps.com/electric-map.html) (click the circle)
- **Large bridges:** E.G., the Four Bears Bridge over the Missouri
- **Interstate railroad lines:** See <http://www.mapsofworld.com/usa/states/north-dakota/maps/north-dakota-railway-map.jpg>
- **Fiber?** See <http://209.62.235.25/uploads/resources/200/fiber.jpg>
- **Frankly, North Dakota is plumb chockablock FULL of non-military critical infrastructure**



## **II. Cyber War Is Not What You Think It Is**

# A Lot of Folks Have Substantial Misconceptions About This "Cyber War" Thing

- -- Cyber war is NOT about “inadvertent” nuclear war
- -- Cyber war is NOT about cyber intrusions
- -- Cyber war is NOT about defacing web sites
- -- Cyber war is NOT about DDoS attacks
- -- Cyber war is NOT about malware
- -- Cyber war is NOT about cyber-enabling regular terrorism
- -- Cyber war is NOT about “high tech” war that isn't computer or network focused, nor is it about “non-technical” military information operations
- That’s all “bad stuff,” and it might be “cyber **espionage**,” or “cyber **terrorism**,” or “**high tech war**” or “**nuclear war**” or “**regular war**” but it’s **not cyber war**. However since a lot of the impressions we have about cyber war are formed around those misconceptions, we need to start by looking at those areas.

### **III. Cyber War $\hat{=}$ Accidental Nuclear War**

## "WarGames" (The Movie)

- Some of you may remember twenty five years ago when there was a well-received movie called “**WarGames**” starring Matthew Broderick as David Lightman, a “war dialing” high school cracker who managed to dial in to WOPR, a NORAD “supercomputer.”
- WOPR was simultaneously both rather loosely-secured and overly-well-connected -- but I don’t want to spoil the movie for you, in the event that you’re one of the millions of folks who may never have seen it or may have seen it but don’t recall it. Speaking of, I’ve brought along a VHS copy of “WarGames;” perhaps Theresa will agree to loan this to those who want to see it?
- **WarGames aside, surely we no longer need to worry about accidental initiation of a global thermonuclear war when we talk about "cyber warfare," and surely random public access to strategic nuclear infrastructure would be impossible -- right? Right?**

# Cyber Attacks and "Inadvertent" Nuclear War

- 'A Real Nuclear Option for the Nominees: Averting "inadvertent" war in two easy steps,' *Slate*, May 9th, 2008, <http://www.slate.com/id/2191104/pagenum/all/> [emphasis added]

*[...] the reason for the 12-minute deadline [for the President to make a launch or don't launch decision] is that missiles launched from offshore submarines can reach coastal targets in less than 15 minutes.*

*So it's insanely short-fused as it is. But when I spoke to [Bruce G.] Blair, ["perhaps the world's leading expert on both the U.S. and the former Soviet Union's nuclear warning and launch postures"] in Washington last week, he noted an additional cause for concern: **cyber-attacks**.*

*He pointed to the preface of his Oslo paper, which focused on **how "information warfare" in cyberspace heightened the threat of "inadvertent" nuclear war.***

*"The nuclear command systems today operate in an intense information battleground," Blair wrote, "on which more than 20 nations including Russia, China, and North Korea have developed dedicated computer attack programs. **These programs deploy viruses to disable, confuse, and delay nuclear command and warning processes in other nations. At the brink of conflict, nuclear command and warning networks around the world may be besieged by electronic intruders whose onslaught degrades the coherence and rationality of nuclear decision-making. The potential for perverse consequences with computer-launched weapons on hair-trigger is clear.**"*

# **“Sample Nuclear Launch While Under Cyber Attack”**



[yes, this is a doctored photo, used here just to lighten a serious moment]

Source: <http://www.armscontrolwonk.com/1955/missile-palooza>

# A Real Case of "Back Door" Access

- Humour noire aside, continuing to quote from 'A Real Nuclear Option for the Nominees: Averting "inadvertent" war in two easy steps':

*"Perverse consequences" seems to understate the matter. In a footnote, Blair cites one scary example: **the discovery of "an unprotected electronic backdoor into the naval broadcast communications network used to transmit launch orders by radio to the U.S. Trident deterrent submarine fleet. Unauthorized persons including terrorists might have been able to seize electronic control of shore-based radio transmitters ... and actually inject a launch order into the network.** The deficiency was taken so seriously that new launch order validation protocols had to be devised, and Trident crews had to undergo special training to learn them."*

*Is this the only "electronic back door"? Or is it just the only one we've discovered? And if an unauthorized launch order could be insinuated into the system by hackers, why not a false-attack warning, which could generate an authorized (but mistaken) launch order? So in addition to the potential for accidental nuclear war, there is an even more disturbing threat of deliberate-but-unauthorized nuclear launches.*

## Serious As Those Issues Are...

- And those *are* quite serious issues, I really don't mean to imply that they're not, we're not here today to talk about accidental nuclear war.
- Accidental nuclear war is “just” nuclear war, **not** cyber war (yes, there are some sorts of national scale cyber warfare which could be more serious than “just” the limited use of nuclear weapons in a conventional albeit inadvertent nuclear attack)
- Okay. But what of the problem of military cyber intrusions by what appears to be a foreign state? Surely **that's** about as obvious a sort of “cyber war” as you can find, right?



## **IV. Military Cyber Intrusions**

# Gary McKinnon's Quest for UFOs (I Kid You Not)

- “British hacker Gary McKinnon in final appeal to Home Secretary over extradition,” [business.timesonline.co.uk/tol/business/law/article4628575.ece](http://business.timesonline.co.uk/tol/business/law/article4628575.ece)  
August 29th, 2008 [emphasis added below]

*[...] Gary McKinnon is due to be extradited to the United States within two weeks and could face a sentence of up to 80 years in a maximum-security prison if found guilty. **He admits to having accessed 97 US Navy, Army, Nasa and Pentagon computers in what has been described as “the biggest computer hack of all time”.***

*Mr McKinnon, 42, an unemployed systems analyst, has said that he was looking for computer files containing details about **UFOs and aliens**. The US Government says that he stole passwords, deleted files and left threatening messages.*

*Mr McKinnon, of Palmers Green, North London, admitted carrying out the hacks using a computer in the bedroom of a house owned by his girlfriend’s aunt. He says that he was motivated by curiosity and gained entry only because of lax security. [...]*

*US prosecutors allege that he caused nearly \$1 million (£550,000) in damage. The US military says that he rendered 300 computers at a US Navy weapons station unusable immediately after the September 11 attacks. [...]*

# Titan Rain

- "The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)," Monday, **Aug. 29, 2005** <http://www.time.com/time/magazine/article/0,9171,1098961,00.html> [emphasis added]

*[...] In Washington, officials are tight-lipped about **Titan Rain**, insisting all details of the case are classified. But high-level officials at three agencies told TIME **the penetration is considered serious**. A federal law-enforcement official familiar with the investigation says the FBI is "aggressively" pursuing the possibility that **the Chinese government is behind the attacks**. Yet they all caution that they don't yet know whether the spying is official, a private-sector job or the work of many independent, unrelated hands. The law-enforcement source says **China has not been cooperating with U.S. investigations of Titan Rain**. China's State Council Information Office, speaking for the government, told TIME the charges about cyberspying and Titan Rain are "totally groundless, irresponsible and unworthy of refute."*

*Despite the official U.S. silence, several government analysts who protect the networks at military, nuclear-lab and defense- contractor facilities tell TIME that **Titan Rain is thought to rank among the most pervasive cyberespionage threats that U.S. computer networks have ever faced**.*

*[continues]*

# A 2006 Estimate of Data Exfiltration: 10-20TB

- *Maj. Gen. William Lord, director of information, services and integration in the Secretary of the Air Force Office of Warfighting Integration and Chief Information Officer, today told an audience of civilian Air Force personnel attending the Air Force IT Conference that "China has downloaded 10 to 20 terabytes of data from the NIPRNet. They're looking for your identity, so they can get into the network as you."*

*Lord said that this is in accordance with the Chinese doctrine about the use of cyberspace in conflict.*

*"We don't think they've gotten into the SIPRNet yet," [the classified GIG network], he said, "though we know they have [penetrated] the NIPRNet. There is a nation-state threat by the Chinese."*

Source: [http://www.gcn.com/online/vol1\\_no1/41669-1.html](http://www.gcn.com/online/vol1_no1/41669-1.html) 20

# 2007 Attacks on the US Defense Department

- **Chinese hacked into Pentagon** ( <http://www.ft.com/cms/s/0/9dba9ba2-5a3b-11dc-9bcd-0000779fd2ac.html> [emphasis added])

*The Chinese military hacked into a Pentagon computer network in June in the **most successful cyber attack on the US defence department**, say American officials.*

*The Pentagon acknowledged shutting down part of a computer system serving the office of Robert Gates, defence secretary, but declined to say who it believed was behind the attack.*

*Current and former officials have told the Financial Times an internal investigation has revealed that the incursion came from the People's Liberation Army.*

*One senior US official said the Pentagon had pinpointed the exact origins of the attack. Another person familiar with the event said there was a "very high level of confidence...trending towards total certainty" that the PLA was responsible. [article continues]*

## So Who *Really* Did It?

- A common problem in looking at cyber intrusions (or other attacks) is that of "attribution," or figuring out **who really did it?**
- First of all, **you may (or may not) be able to trace an attack or an intrusion to a system in a particular country** -- some types of traffic (such as UDP traffic) can be trivial to spoof.
- If you do succeed in tracing an attack back to a particular system, and it happens to hypothetically be in China, **it may also have been subject to a cyber intrusion**, and may just be acting as a "stepping stone" for a real attacker located somewhere else. There may even be a **series or "chain" of stepping stones** in use
- Let's assume, however, that you do succeed in identifying the location of the system that originated the attack. **Just because a system might be physically in Russia, for example, doesn't mean that the Russian government has authorized or initiated the attack that you hypothetically saw from that computer.**
- In fact, you need to be alert to intentional attempts at cyber deception.

# Hypothetical Attempts at Deception

- Pro-Taiwan activists (wanting to sour relations between the United States and China) might launch cyber attacks against US targets that seem to be coming from the People's Republic, hoping that the mainland Chinese government would get blamed for them.
- China itself might actually launch cyber attacks from its own territory against the United States, but when questioned about that activity, might then blame those attacks on "Taiwanese hackers" (who might actually have had nothing to do with it whatsoever).
- Russian nationals, living in the US, might purchase access to a server in Amsterdam, using a stolen credit card in Spain, and then use that server to stage intrusions on Georgian systems...
- You see the sort of "attribution problems" that can arise, right?
- This is **not** to say that attribution is **always** impossible, because sometimes attacks **can** be successfully backtracked.
- Other times, things like official cooperation (or a lack thereof) when investigating a cyber attack can tell you a lot about who may be ultimately responsible.

**V. Cyber War = Defaced Websites?**



# Digital Graffiti

## U.S.-China cyberwar a dud, but trouble lingers

Sam Costello, IDG News Service

---

May 11, 2001 ([IDG News Service](#)) What if they waged a cyberwar and nobody came?

That seems to be the situation after the end of what was described as a cyberwar staged by Chinese hackers against the U.S. in retaliation for the death of Chinese pilot Wang Wei in early April. Doubts linger in some Internet security experts' minds, however, about whether this cyberwar was the week's real threat.

A Chinese hacker group, the Honker Union of China, issued a statement to the Chinese portal site Chinabyte earlier this week declaring a truce, saying it had hacked 1,000 U.S. sites.

But a truce was perhaps unnecessary, as nothing approaching a war ever materialized during the 10 days after the FBI's National Infrastructure Protection Center issued a warning saying Chinese hackers would attack U.S. Web sites between April 30 and May 7 ([see story](#)).

Rather, the only traces of a conflict were, on one hand, a series of Web page defacements that included pictures of Wang Wei -- who died when his plane crashed into a U.S. spy plane -- and promises to fight "hegemony" and to "unify the motherland," and, on the other, a good deal of anti-Chinese sentiment from American hackers.

Web page defacements are a form of slightly sophisticated digital graffiti that involve a hacker leaving a message or an image on a Web site to show that its security has been breached. This sort of attack, however, is equivalent to "pouring paint on some ... person's building," said Alan Paller, director of security research at the [SANS Institute](#) in Bethesda, Md.

# Defacements Don't Need to Be “Dramatic:”

## A Few Words Are Enough to Prove That A Breach Happened And That Remediation Will Be Needed

Mirror saved on: 2008/05/15 23:16		
Defacer: ISCN	Domain: http://namru3.med.navy.mil/Portals/0/ISCN.txt	IP address: 205.73.217.15
System: Win 2003	Web server: IIS/6.0	Attacker stats

Owned By : Magic-Boy And Imm02tal  
Contact Us : ISCNltd@GMail.coM  
ISCN Team

Source: [http://www.zone-h.org/component/option,com\\_mirrorwrp/Itemid,160/id,7464025/](http://www.zone-h.org/component/option,com_mirrorwrp/Itemid,160/id,7464025/)

# Some Defacements, However, May Be Less Subtle


Zone-H.org - Unrestricted Information - dodtravelregs.hqda.pentagon.mil defaced by Agd\_Scorp

http://www.zone-h.org/component/option,com\_mirrorwrp/Itemid,0/id,777 Google

Wednesday, 10 September 2008

Mirror saved on: 2008/08/18 01:30		
Defacer: Agd_Scorp	Domain: http://dodtravelregs.hqda.pentagon.mil/t	IP address: 141.116.10.20
System: Win 2003	Web server: Unknown	Attacker stats

**Terrorist Crew**



~ Hi Master ~

Hacked by | Agd\_Scorp , JeXToXiC , Wh0!, Starturk, Rx5, AntiW4R, Security-Terror

Gr33t3 to : Kerem125, Gov, Oscar-Sanders, CoBB@il, The Bekib, al-CD

# Decomposing A Web Site Defacement

- A web site defacement consist 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?

# Objectives Behind Web Site Defacements

- Defacements may be done in an effort
  - to publicly “strike a blow” against a perceived enemy
  - to embarrass a targeted site by illustrating a security issue
  - to attract public attention to a cause, an “injustice,” or an entity
  - to challenge/deny informal web server use by an organization
  - to reduce public confidence in the security of a system and its trustworthiness for use for sensitive purposes
  - to force a targeted system to be taken out of service until it can be scrutinized/analyzed, formatted, rebuilt, and hardened
  - to establish “street cred” with one’s hacker/cracker peers, or
  - simply because the defacer finds doing defacements to be “fun”
- To achieve most of these ends, defacements done by a hacker/cracker **must be noticed**. However, once a defacement is noticed, **the defaced site will usually get taken off line** and the defacement will **disappear** (except for potential archived copies).

# Defacement: Cyber War, or Cyber Terrorism?

- Is defacing a web site cyber war, or is it a sort of cyber terrorism?
- I'd argue it is actually cyber terrorism, not cyber war. A test to potentially help you decide: does a web site defacement **rely on publicity/public attention for its effects**? Or would it be an equally potent attack if the media ignored it? I believe web site defacements **only** “work” if people notice a defacement occurred.
- Remember: every web site defacement implies at least some degree of unauthorized access. **Intentionally** drawing attention to a compromised machine by putting up a defaced web page means that **the attacker is willing to forgo *sub rosa* exploitation of that system in exchange for public attention**. If the attacker had NOT done a public defacement, that compromised system might have remained usable as a stepping stone, or as an ongoing source of intelligence, etc. Once a defaced web page is put up, it becomes clear that that system has been 0WN3D, and it will get fixed.

# The Fundamental Problem of Cyber Terrorism

- **The biggest and most fundamental problem facing a potential cyber terrorist is that often they can't rise above the normal online "noise floor."**
- Someone take a favorite web site offline? "Hmm. Something must be broken. I guess I'll have to try it again later."
- Hacked system? New malware? DDoS? Well, with hacked system after hacked system, and new piece of malware after new piece of malware, and DDoS after DDoS, there's not much "shock value" left when it comes to "terroristic" cyber hacking.
- Fundamentally, spammers, aggressive online advertisers, scammers and phishers have done a fine job of training the general public to cynically tune out most unwanted or discordant "push" communications, so when confronted with a terrorist's message, the public is liable to view it with a critic's eye, if at all ('oh look, they misspelled "oppressor" again'), and then just surf right on by.

## **VI. Distributed Denial of Service Attacks**



# “Cyber War” In Estonia, 2007

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

BBC NEWS | Europe | Estonia hit by 'Moscow cyber war'

http://news.bbc.co.uk/2/hi/europe/6665145.stm

Last Updated: Thursday, 17 May 2007, 15:21 GMT 16:21 UK

[E-mail this to a friend](#) [Printable version](#)

## 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.



Estonia says many state websites have been affected

## 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.

-----

\* If you're not familiar with DDoS attacks, I discuss them, and some implications associated with them, in:

"Explaining Distributed Denial of Service Attacks to Campus Leaders,"  
May 3, 2005, <http://www.uoregon.edu/~joe/ddos-exec/ddos-exec.pdf> (80 slides)

# **Some People, Including Estonia Itself, Eventually Had Doubts About This "Cyber War"**

- Kevin Poulsen, **“Estonia Drops Cyberwar Theory, Claims Packets Were 'Terrorism',”** June 7, 2007,  
[http://blog.wired.com/27bstroke6/2007/06/estonia\\_drops\\_c.html](http://blog.wired.com/27bstroke6/2007/06/estonia_drops_c.html)  
See also Polson’s: **“'Cyberwar' and Estonia's Panic Attack,”**  
<http://blog.wired.com/27bstroke6/2007/08/cyber-war-and-e.html>  
August 22, 2007
- Gary Warner, **‘Evidence that Georgia DDOS attacks are "populist" in nature,’** <http://garwarner.blogspot.com/2008/08/evidence-that-georgia-ddos-attacks-are.html>
- Jose Nazario, **“Estonian DDoS Attacks - A summary to date,”**  
<http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/>

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

BBC NEWS | Technology | Estonia

  <http://news.bbc.co.uk/2/hi/technology/7208511.stm>

## 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.



The attacks were in response to the relocation of a war memorial

# 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](http://www.president.gov.ge)) and the website for the Parliament of Georgia ([www.parliament.ge](http://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](http://www.president.gov.ge)  
[www.parliament.ge](http://www.parliament.ge)  
[apsny.ge](http://apsny.ge)  
[news.ge](http://news.ge)  
[tbilisiweb.info](http://tbilisiweb.info)  
[newsgeorgia.ru](http://newsgeorgia.ru)  
[os-inform.com](http://os-inform.com)  
[www.kasparov.ru](http://www.kasparov.ru)  
[hacking.ge](http://hacking.ge)  
[mk.ru](http://mk.ru)  
[newstula.info](http://newstula.info)  
[skandaly.ru](http://skandaly.ru)

# “Georgia Cyberwar Overblown”

- *There are two problems with the theory of cyberwarfare in the Caucasus. 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.*

Source: “Georgia Cyberwar Overblown,” Andreas Antonopoulos, 8/19/2008  
<http://www.networkworld.com/columnists/2008/081908-andreas.html> [emphasis added]



# 4/16/2008: A Government, Unhappy With CNN...

[http://news.xinhuanet.com/english/2008-04/16/content\\_7988422.htm](http://news.xinhuanet.com/english/2008-04/16/content_7988422.htm)



Chinese Foreign Ministry spokeswoman Jiang Yu  
[Photo Gallery>>>](#)

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 hundred 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 50 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)

# Followed By “People’s Information Warfare”

- Wednesday, **April 23rd, 2008**, “DDoS Attack Against CNN.com,” [ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html](http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html) [emphasis added below]

“The DDoS attack against CNN.com, whether successful or not in terms of the perspective of complete knock-out, which didn't happen, **is a perfect and perhaps the most recent example of a full scale people's information warfare in action.** [...]

“[...] Estonia's DDoS attacks were a combination of botnets and DIY attack tools released in the wild, whereas **the attacks on CNN.com were primarily the effect of people's information warfare, a situation where people would on purposely infect themselves with malware released on behalf of Chinese hackers to automatically utilize their Internet bandwidth for the purpose of a coordinated attack against a particular site.**”  
[continues]



# Another Recent DDoS Against a News Site...

- *Various news sources are reporting that Radio Freedom Europe's Belarus site was DDoS'ed this weekend starting from April 26. The radio station was going to cover mass protests in Minsk, Belarus dedicated to the anniversary of the Chernobyl disaster. The radio station had plans to direct people to their website to check out pictures, videos of the coverage, etc. However, much to their dismay their site was totally inaccessible for 2 days and 2 nights under a massive DDoS storm. According to the RFE/RL Belarus Service Director:*

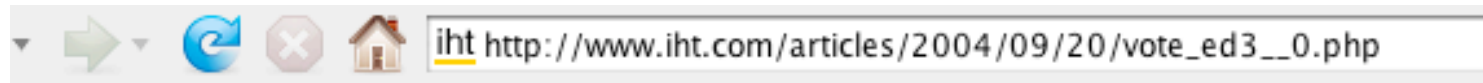
*“There was not much we could do because at this moment we also lost e-mail communication and Skype communication with Belarus. As we found out later, the attack was so massive that the firewall that protects Radio Free Europe went down. And a number of other [RFE/RL] sites went down as well.”*

# Is There Nothing That Can Be Done?

## A 1999 DDoS Counter-Offensive

- "Cyber-Civil Disobedience," 01/11/99,  
<http://www.networkworld.com/news/0111vigcyber.html> [emphasis added]  
*The battle between the Electronic Disturbance Theater (EDT) and the Pentagon is a potential watershed event: **The first time - that we know of - that the U.S. military launched a cyber counter-offensive** against people within the United States.*  
*On September 9, 1998, the EDT launched a denial of service program called FloodNet against a Pentagon Web site. "Floodnet causes persistent re-searching of the targeted site's local search engine every nine seconds," says EDT member Ricardo Dominguez. Essentially, it chews up CPU time and resources.*  
*Dominguez and the EDT call their cyber-protest performance art on the Internet, meant to focus on the plight of the Zapatistas, a rebel group that supports the rights of Indians in Chiapas, Mexico. Because the U.S. supports the Mexican government in opposing the Zapatistas, the EDT considers the Pentagon a legitimate target.*  
*According to highly placed Pentagon sources, the Floodnet assault was pre-announced by the EDT so the Pentagon was able to prepare for it. Its response was orchestrated by the Defense Information Systems Agency (DISA), which has experience with both defensive and offensive cyber-tools.*  
*Once the attack began, the Pentagon launched a denial of service attack of its own. Requests from the EDT browsers were redirected to a Java applet called 'hostileapplet,' which Dominguez says crashed the browsers. The applet fired a "series of rapidly appearing Java coffee cups across the bottom of the browser screen coupled with the phrase 'ACK.' FloodNet froze," he says.*

# A 2004 Try At Filtering Unwanted Hacker Traffic



## Pentagon blocks site for voters outside U.S.

By Jennifer Joan Lee

Published: MONDAY, SEPTEMBER 20, 2004

**PARIS:** In a decision that could affect Americans abroad who are not yet registered to vote in the Nov. 2 presidential election, the Pentagon has begun restricting international access to the official Web site intended to help overseas absentee voters cast ballots.

According to overseas-voter advocates who have been monitoring the situation, Internet service providers in at least 25 countries — including Yahoo Broadband in Japan, Wanadoo in France, BT Yahoo Broadband in Britain and Telefónica in Spain — have been denied access to the site of the Federal Voting Assistance Program, apparently to protect it from hackers.

In an e-mail addressed to a person in France who had tried to access the Web site, the Federal Voting Assistance Program's Web manager, Susan Leader, wrote: "We are sorry you cannot access [www.fvap.gov](http://www.fvap.gov). Unfortunately, Wanadoo France has had its access blocked to U.S. government Web sites due to Wanadoo users constantly attempting to hack these sites. We do not expect the block to be lifted."

In Washington, a Pentagon spokeswoman reached by telephone confirmed that a number of Internet service providers worldwide had been blacklisted to thwart hackers. The spokeswoman, Lieutenant Colonel Ellen Krenke, declined to comment further.

# Example of a Current Generation DDoS Attack

- Not all potential DDoS targets are web based. For example, for a discussion of large-scale DDoS attacks targeting DNS, see:
  - “SSAC Advisory SAC008 DNS Distributed Denial of Service Attacks,” <http://www.icann.org/en/committees/security/dns-ddos-advisory-31mar06.pdf>
  - “Factsheet: Root Server Attack on 6 February 2007”  
[http://www.icann.org/en/announcements/factsheet-dns-attack-08mar07\\_v1.1.pdf](http://www.icann.org/en/announcements/factsheet-dns-attack-08mar07_v1.1.pdf)
  - pp. 22 of Jose Nazario’s “Political DDoS: Estonia and Beyond,”  
[www.usenix.org/events/sec08/tech/slides/nazario-slides.pdf](http://www.usenix.org/events/sec08/tech/slides/nazario-slides.pdf)
- To date, due in large part to DNS caching, long DNS TTLs, and widespread deployment of replicated "anycast" root name server nodes, attempts at DDoS'ing the root name servers have generally had limited operational impact.

# How NOT To Do A DDoS/Counter-DDoS

- See "Carpet Bombing In Cyberspace: Why America needs a military botnet," [www.armedforcesjournal.com/2008/05/3375884](http://www.armedforcesjournal.com/2008/05/3375884) I quote from that article:  
*The U.S. would not, and need not, infect unwitting computers as zombies. We can build enough power over time from our own resources. Rob Kaufman, of the Air Force Information Operations Center, suggests mounting botnet code on the Air Force's high-speed intrusion-detection systems. Defensively, that allows a quick response by linking our counterattack to the system that detects an incoming attack. The systems also have enough processing speed and communication capacity to handle large amounts of traffic.*
- One's mind boggles for many reasons that someone would propose this. The real power of bots/zombies in a DDoS comes from the fact that they are NOT all just in a single autonomous system number or a small set of ASNs, they're all over the place, and more importantly, there's REAL stuff associated with those same IP addresses and those same ASNs (which means you can't, or don't want to just summarily drop those parts of the Internet).
- If af.mil built and homed a botnet inside of its normal operations, voila, Kerblechistan or whatever we might target with that af.mil "botnet" could just drop any traffic from the af.mil ASNs (jeez, how hard would it be to develop \*that\* incredibly complex defensive strategy, eh?)

# By Tricking You Into Attacking The Wrong Sort of Targets, Bad Guys Can Multiply Their Power

- From: n3td3v <xploitable at gmail.com>  
Date: Wed, May 21, 2008 at 11:25 AM  
Subject: Re: [Full-disclosure] pentagon botnet  
To: full-disclosure at lists.grok.org.uk

On Wed, May 21, 2008 at 9:16 AM, S/U/N <s.u.n at free.fr> wrote:  
> <http://www.afji.com/2008/05/3375884/>

What if the bot net of the enemy state are hospital computers, will you still attack them? What if the bot net of the enemy state are power station computers, will you still attack them? Will you risk putting civilian life at risk if the enemy state hides their bot net in national infrastructure that will make you look the worst if you attack them?

Enemy states would end up hiding their bot nets in places you wouldn't want to attack... because if you did it would shut down a national infrastructure. The enemy states aren't going to have their bot nets in home computers with Windows Vista running, they are going to be national infrastructure computers that if you attack them will put the countries civilians at risk, making you the baddies and them the goodies. [post continues]

# Trusted Internet Connection Program

- Before we leave the topic of distributed denial of service attacks, let me also draw your attention to the Trusted Internet Connection (TIC) Program. Under the TIC program, the Federal Government is working to take the number of interconnections between federal agencies and the Internet down from thousands to just fifty (50).
- While reducing the number of points of interconnection may reduce the number of such connections which are poorly monitored (or unmonitored), reducing the number of network connections may perversely potentially serve to **increase** the vulnerability of federal networks to DDoS attacks.
- If you're interested, please can see my discussion of this in "Cyberinfrastructure Architectures, Security and Advanced Applications" from the April 2008 Internet2 Member Meeting, <http://www.uoregon.edu/~joe/architectures/architecture.pdf> slides 85-92

## **VII. Malware and "Cyber War"**



# A "Classic" "Cyber War" Weapon: "Viruses"

- Another presumptive weapon of cyber war: "viruses" (actually a range of malware such as computer viruses, network worms, trojan horses, root kits, spyware, etc.).
- The US Department of Defense believes that at least some nations have active military virus development capabilities:

The PLA has established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks. In 2005, the PLA began to incorporate offensive CNO into its exercises, primarily in first strikes against enemy networks.

<http://www.defenselink.mil/pubs/pdfs/070523-China-Military-Power-final.pdf>  
[The CNO in the above quotation stands for "Computer Network Operations"]

# May 2008 Hearings of the US-China Economic and Security Review Commission

- “[...] when I say reduce our exposure, these are the sorts of things on this slide that we want to try to minimize in terms of making their way on to DoD networks, things like root kits, virus/worms, spyware/adware, and **the most difficult one that we're all facing, both on the industry side as well as the U.S. government side, are socially engineered e-mail or phishing attacks**, very difficult problem today, especially for folks that are able to really do reconnaissance and understand an organization, their TTPs [tactics, techniques and procedures], how they do business. They understand the people in those organizations so that **when you or I receive an e-mail that looks like it's coming from our boss, why wouldn't we open it?**

**“And in many cases, that socially-engineered e-mail has malicious software or payload that takes you to a site that allows you to be compromised, many times unbeknownst to you.”**

“Hearing on “China’s Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities,”

[http://www.uscc.gov/hearings/2008hearings/transcripts/08\\_05\\_20\\_trans/08\\_05\\_20\\_trans.pdf](http://www.uscc.gov/hearings/2008hearings/transcripts/08_05_20_trans/08_05_20_trans.pdf)

# Like China, The USAF Is Interested In Malware

- “**Dominant Cyber Offensive Engagement and Supporting Technology**,” BAA-08-04-RIKA, May 12th, 2008, [https://www.fbo.gov/index?s=opportunity&mode=form&Id=b34f1f48d3ed2ce781f85d28f700a870&tab=core&\\_cview=0&cck=1&au=&ck](https://www.fbo.gov/index?s=opportunity&mode=form&Id=b34f1f48d3ed2ce781f85d28f700a870&tab=core&_cview=0&cck=1&au=&ck) [emphasis added below]

*Solutions to basic and applied research and engineering for the problems relating to **Dominant Cyber Offensive Engagement and Supporting Technology** are sought. This includes high risk, high payoff capabilities for **gaining access to any remotely located open or closed computer information systems; these systems enabling full control of a network for the purposes of information gathering and effects based operations.** Of interest are any and all techniques to enable user and/or root level access to both fixed (PC) or mobile computing platforms. Robust methodologies to enable access to any and all operating systems, patch levels, applications and hardware are of interest. Also, **we are interested in technology to provide the capability to maintain an active presence within the adversaries' information infrastructure completely undetected.** Of interest are any and all techniques to enable stealth and persistence capabilities on an adversaries infrastructure. This could be a combination of hardware and/or software focused development efforts.*

- *Following this, it is desired to have the capability to **stealthily exfiltrate information from any remotely-located open or closed computer information systems with the possibility to discover information with previously unknown existence.** Any and all techniques to enable exfiltration techniques on both fixed and mobile computing platforms are of interest. Consideration should be given to maintaining a **"low and slow" gathering paradigm in these development efforts to enable stealthy operation.** Finally, this BAA's objective includes the capability to provide a variety of techniques and technologies to be able to **affect computer information systems through Deceive, Deny, Disrupt, Degrade, Destroy (D5) effects.** Of interest are any and all techniques including enabling D5 effects to computers and their networks; integration of effects with Access, Stealth and Persistence and Cybint capabilities; command and control of effects; and determining effects link to operational impact. In addition to these main concepts, we desire to have [BAA continues]*

# What Do Some People Think of That?

## NSA vs. USAF

- *A senior Pentagon official said that "exploiting" computer networks to gather intelligence is currently the most important use of cyber-power. "Clearly, the exploitation activities have been preeminent," the official said.*

*[...]*

*"Let's not mistake intelligence collection with military operations," said Lani Kass, a senior Air Force official and former director of the service's Cyberspace Task Force. "The mission of the NSA is to collect signals intelligence, and it is very good at it. But the NSA is not a war-fighting organization."*

*"Pentagon debates development of offensive cyberspace capabilities," Los Angeles Times, September 8th, 2008  
<http://www.latimes.com/news/printedition/front/la-na-cyber8-2008sep08,0,909623.story>*

# Bureaucratic Shoals: USAF vs. the Navy and Army

- **Air Force suspends Cyber Command program (08/12/08)**  
[http://www.nextgov.com/nextgov/ng\\_20080812\\_7995.php](http://www.nextgov.com/nextgov/ng_20080812_7995.php) [emphasis added]

*The Air Force on Monday suspended all efforts related to development of a program to become the dominant service in cyberspace, according to knowledgeable sources. Top Air Force officials put a halt to all activities related to the establishment of the Cyber Command, a provisional unit that is currently part of the 8th Air Force at Barksdale Air Force Base in Louisiana, sources told Nextgov.*

*An internal Air Force e-mail obtained by Nextgov said, “Transfers of manpower and resources, including activation and reassignment of units, shall be halted.” Establishment of the Cyber Command will be delayed until new senior Air Force leaders, including Chief of Staff Norton Schwartz, sworn in today, have time to make a final decision on the scope and mission of the command.*

*The Cyber Command, headed by Maj. Gen. William Lord, touted on its Web site its capabilities to “secure our nation by employing world-class cyberspace capabilities” and had ambitious plans to have a cyber command presence in all 50 states.*

*The Cyber Command hyped its capabilities on TV, in Web video advertisements and in a series of high-profile presentations conducted by Lord. **The hard sell may have been the undoing of the Cyber Command, which seemed to be a grab by the Air Force to take the lead role in cyberspace. Both the Army and Navy have similar expertise in cyber operations, service sources said.** [article continues]*

# More Turf Battles: DHS vs. NSA vs. White House

September 19, 2008 10:20 AM PDT

## Should NSA take over federal cybersecurity efforts?

Posted by [Stephanie Condon](#)

[2 comments](#)

 [Print](#)  [E-mail](#)  [Share](#)

Political pressure is mounting to eliminate the U.S. Department of Homeland Security's lead role over cybersecurity, a move that that would effectively admit the agency's failure to adequately perform its assigned duties.

But that invites the obvious question: Who should take over? One option would be, as we [heard earlier this week](#), the White House itself. Another choice would be the more shadowy world of intelligence agencies such as the CIA or National Security Agency, which already [is responsible for](#) protecting government computers through its "information assurance" arm.

All week, members of a cybersecurity commission forming recommendations for the next administration have been [telling Congress](#) that cybersecurity requires senior level policy and program coordination from the White House.

Even though Homeland Security [claims](#) that cybersecurity is one of its top priorities, the department is not equipped to handle cyberthreats, says the Center for Strategic and International Studies' [Commission on Cybersecurity for the 44th Presidency](#), a private effort that [includes representatives](#) of the so called "intelligence community."



Source: [http://news.cnet.com/8301-13578\\_3-10045980-38.html](http://news.cnet.com/8301-13578_3-10045980-38.html)

# “Cyber War” Should NOT Refer to Which Federal Agency Will Get to Be In Charge of Cybersecurity!

- Postulated for the sake of discussion:
  - the United States has compelling national interests online
  - those interests may variously be scientific, economic, political, military, national security-related, etc.
  - government cyberspace-related operations may involve federal law enforcement; any or all of the military branches; any or all agencies of the national intelligence community; as well as state and local law enforcement; international partners; Internet-related and non-Internet-related businesses; etc.
  - if we’re unable to collaborate and work together, we’re only hurting the United States and helping our common enemies
  - we’ve still got a **lot** of work still ahead of us, so...

**==> The fighting “within the family” has got to stop.**

# Coming Back to Malware: Is Malware Even Really A Suitable Tool for Cyber Warfare?

- Malicious code, such as computer viruses, worms, trojan horses, spyware, etc., obviously represents a huge ongoing nuisance to many desktop systems, but just like a defaced web site, an infested enterprise desktop or laptop can be taken offline, rebuilt, hardened and redeployed: it normally won't be permanently damaged.\*
- It is true that a malware-compromised system may represent a vector for data leakage/intelligence collection, but remember, *cyber espionage isn't cyber war*.
- Malware also has some serious challenges as a weapon of cyber warfare. For example...

----

Potential exception: Weaver and Paxson's "Worst Case Worm:"  
<http://www.icir.org/vern/papers/worst-case-worm.WEIS04.pdf>  
discusses potential widespread damage to firmware



# Exploits: Perishable Assets With Short Shelf Lives

- Computer malware which leverages heretofore unknown vulnerabilities is a “wasting asset.” Having found a vulnerability, assume an exploit is developed to take advantage of it. If that exploit doesn’t get used, but just gets “put in the stockpile” for potential later use, it’s value will likely **drop over time**. Why?
  - A vendor, a security researcher, or a hacker/cracker may spontaneously re-discover “your” vulnerability and patch it (or use it!) before you do, making “your exploit” into a “dud,” one which is easily identified (and blocked) if it still works at all
  - Obsolescence of associated software products may also occur (e.g., exploits for W/95 or W/98 aren’t very relevant any more)
- So by implication, if a military virus writing unit *did* discover a vulnerability and developed an exploit to take advantage of it, that asset would have an implicit cyber “best if used by” date and associated pressure to “use it” before you “lose it.” But what if you aren’t currently engaged in a cyber conflict, eh? Tick, tock.<sup>17</sup>

# Other Problems With “Weaponizing” Malware

- Let’s not overlook the “**shifting wind**” or “**boomerang**” problem: computer malware, like traditional chemical or biological warfare agents, can potentially “get away from you,” drifting off course or “boomeranging back,” accidentally hitting one’s own forces or allies or hitting uninvolved third parties, rather than the enemy.
- However, if malware can learn to reliably distinguish “friends” from “foes,” unintended potential side effects may be able to be contained, and inhibitions (which might otherwise deter potential use) may be lowered or eliminated.
- For example, hypothetically imagine:
  - a localization-aware worm that wouldn’t attack systems if those systems are using a particular **language** or **character set**
  - infrastructure-targeting malware which only attacks hardware from vendor C (commonly used in a targeted country) while hypothetically ignoring hardware from vendor H (commonly used primarily by the attacking country and its allies)

# Firewalls As Protection from Military Malware?

- Some countries, such as China, may believe that a national firewall, such as the Chinese “Golden Shield,” will protect them from any malware which may be targeting them. See, for example, “China’s Golden Shield,”  
[http://www.forbes.com/security/2007/07/30/china-cybercrime-war-tech-cx\\_ag\\_0730internet.html](http://www.forbes.com/security/2007/07/30/china-cybercrime-war-tech-cx_ag_0730internet.html) :

*If China did turn computer viruses into a military tool, the Golden Shield could be used to prevent collateral damage, says Jayson Street, a member of the Netragard SNOsoft Research Team and consultant for Stratagem 1 Solutions. "The firewall would protect China from whatever it releases," says Street. "When a worm goes out, it's not a gun, it's a bomb. It affects everyone. That's why the Golden Shield could be so effective."*

## **But Would Those Firewalls Be Completely And Hermetically “Air Tight”?**

- While the Golden Shield or equivalent national-scale content control systems might be able to detect and block some malware, it is **not** clear to me that any national scale (or even regional scale) firewall could reasonably be counted on to be absolutely “leak proof.” And once malware manages to get a toehold inside that perimeter, well, then it could propagate very rapidly...
- For proof-by-demonstration of the proposition that the Golden Shield is not in fact “air tight,” consider readily available anti-censorship circumvention networks, such as those associated with UltraReach (see <http://www.ultrareach.com/> ). As described on the next page, Ultrareach is currently used by millions of individuals who live in areas where access to the Internet is controlled. Any (or all!) of those millions of anti-censorship circumvention network user might potentially serve as a conduit through which malware from outside China might penetrate to the inside of regions nominally “protected” by the Golden Shield.

- “**Testimony of Shiyu Zhou, Ph. D.,**” May 20, 2008  
[http://judiciary.senate.gov/hearings/testimony.cfm?id=3369&wit\\_id=7187](http://judiciary.senate.gov/hearings/testimony.cfm?id=3369&wit_id=7187) [emphasis added]

*[...] For more and more users around the world, [...] proper anti-censorship technology means tools like **FreeGate** and **UltraSurf** -- created by the **Global Internet Freedom Consortium** (GIF), a small team of dedicated men and women, connected through their common practice of **Falun Gong**, who have come together to battle tens of thousands of Internet monitors and censors around the world to work for the cause of Internet freedom. [...] The Consortium provides its products and support services to those citizens entirely **free of charge**. [...]*

*Our five existing tools – UltraSurf, DynaWeb FreeGate, Garden, GPass, and FirePhoenix – currently accommodate an estimated **95% of the total anti-censorship traffic in closed societies around the world**, and are used **DAILY** by **millions of users**. These tools have been of benefit to US-based organizations such as Human Rights In China, the Chinese Democracy Party, Voice of America, and Radio Free Asia -- and even companies like Google and Yahoo since we bring the uncensored version of their services into closed societies like China.*

*As of January 2008, the Top Five censoring countries with the most average daily hits to our anti-censorship systems are (hits per day): (a) China: 194.4 million, (b) Iran: 74.8 million, (c) Saudi Arabia: 8.4 million, (d) UAE: 8 million, (e) Syria: 2.8 million.*

*[...] we thank Senator Leahy, Senator McConnell, Senator Gregg, Congresswoman Lowey, and Congressman Wolf, for the **Internet freedom initiative in the fiscal year 2008 Foreign Operations Appropriations Bill** which set up a competition for a **\$15 million grant** for "field-tested" Internet technology programs and protocols that, in the words of the appropriation legislation, "have the capacity to support large numbers of users simultaneously in a hostile internet environment."*

# Some Simple Defenses May Help to Mitigate Commonly Seen Malware

- **“DOD bars use of HTML e-mail, Outlook Web Access,”**  
<http://www.fcw.com/online/news/97178-1.html>  
December 22, 2006
- **“Apples for the Army,”**  
[http://www.forbes.com/home/technology/2007/12/20/apple-army-hackers-tech-security-cx\\_ag\\_1221army.html](http://www.forbes.com/home/technology/2007/12/20/apple-army-hackers-tech-security-cx_ag_1221army.html)  
December 21, 2007:

*Though Apple machines are still pricier than their Windows counterparts, the added security they offer might be worth the cost, says Wallington. He points out that Apple's X Serve servers, which are gradually becoming more commonplace in Army data centers, are proving their mettle. "Those are some of the most attacked computers there are. But the attacks used against them are designed for Windows-based machines, so they shrug them off," he says.*

# But Is Malware Even the Real Issue?

- “High Performance Microchip Supply,” February 2005,  
[http://www.acq.osd.mil/dsb/reports/2005-02-HPMS\\_Report\\_Final.pdf](http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final.pdf)

*The Department of Defense and its suppliers face a major integrated circuit supply dilemma that threatens the security and integrity of classified and sensitive circuit design information, the superiority and correct functioning of electronic systems, system reliability, continued supply of long-system-life components, and special technology components.*

- “Mission Impact of Foreign Influence on DoD Software,” September 2007,  
[http://www.acq.osd.mil/dsb/reports/2007-09-Mission\\_Impact\\_of\\_Foreign\\_Influence\\_on\\_DoD\\_Software.pdf](http://www.acq.osd.mil/dsb/reports/2007-09-Mission_Impact_of_Foreign_Influence_on_DoD_Software.pdf)

*The Intelligence Community (IC) does not adequately collect and disseminate intelligence regarding the intents and capabilities of nation-state adversaries to attack and subvert DoD systems and networks through supply chain exploitations, or through other sophisticated techniques.*

## More Bluntly Put...

- **“Pentagon Worries About Chinese Chips,”** Sept 4th, 2008, [http://www.forbes.com/2008/09/04/pentagon-defense-contractors-biz-wash-cz\\_atg\\_0904beltway\\_print.html](http://www.forbes.com/2008/09/04/pentagon-defense-contractors-biz-wash-cz_atg_0904beltway_print.html)

*"The defense community is critically reliant on a technology that obsolesces itself every 18 months, is made in [i]nsecure locations and over which we have absolutely no market share influence," said Ted J. Glum, director of the DoD's Defense Microelectronics Activity unit.*

*"Other than that," he cracked, "we're good."*



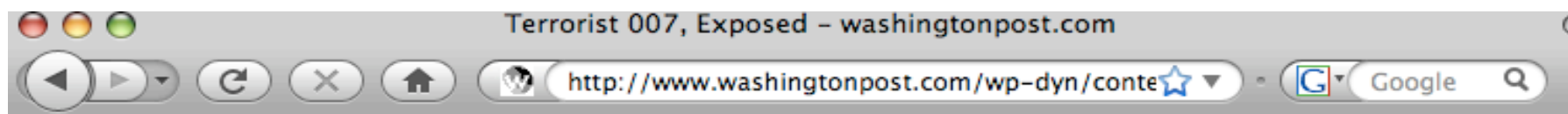
# Tracking Chinese Hacking: The Dark Visitor

- One of the consistently best sources of data on Chinese hacking is Scott J. Henderson's "The Dark Visitor," see <http://www.thedarkvisitor.com/>

It's author describes himself as, "Retired from the US Army after 20 years of service in the intelligence community as a Chinese linguist. I hold a Bachelor of Science degree with an emphasis on Chinese studies and graduated from the Defense Language Institute in Monterey California. In 2006, I attended the XCon2006 computer security seminar held in Beijing China and in 1997 was on special assignment to the US Embassy in the People's Republic of China. One of my fondest memories was attending the Beijing Institute of Economic Management Immersion Program in 1995."

- "The Dark Visitor" is a site well worth routinely reading.

# **VIII. Cyber War is NOT About "Cyber-Enabling" Regular Terrorism**



washingtonpost.com

NEWS | OPINIONS | SPORTS | ARTS & LIVING | Discussions | Photos & Video | City Guide | CLASSIFIEDS | JOBS | CARS | REAL ESTATE

## Terrorist 007, Exposed

Advertisement

By Rita Katz and Michael Kern  
Sunday, March 26, 2006; B01

For almost two years, intelligence services around the world tried to uncover the identity of an Internet hacker who had become a key conduit for al-Qaeda. The savvy, English-speaking, presumably young webmaster taunted his pursuers, calling himself Irhabi -- Terrorist -- 007. He hacked into American university computers, propagandized for the Iraq insurgents led by Abu Musab al-Zarqawi and taught other online jihadists how to wield their computers for the cause.

Suddenly last fall, Irhabi 007 disappeared from the message boards. The postings ended after Scotland Yard arrested a 22-year-old West Londoner, Younis Tsouli, suspected of participating in an alleged bomb plot. In November, British authorities brought a range of charges against him related to that plot. Only later, according to our sources familiar with the British probe, was Tsouli's other suspected identity revealed. British investigators eventually confirmed to us that they believe he is Irhabi 007.

The unwitting end of the hunt comes at a time when al-Qaeda sympathizers like Irhabi 007 are making explosive new use of the Internet. Countless Web sites and password-protected forums -- most of which have sprung up in the last several years -- now cater to would-be jihadists like Irhabi 007. The terrorists who congregate in those cybercommunities are rapidly becoming skilled in hacking, programming, executing online attacks and mastering digital and media design -- and Irhabi was a master of all those arts.

[http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2006/03/25/AR2006032500020_pf.html)

# **The Case of United States of America v. Daniel Joseph Maldonado a/k/a Daniel Aljughaifi**

- Background reading about Joseph Maldonado...
- "American Is Charged in U.S. for Activities in Somalia,"  
<http://www.washingtonpost.com/wp-dyn/content/article/2007/02/13/AR2007021301164.html>
- "Superseding Criminal Complaint," Case Number H-07-125M,  
[www.foxnews.com/projects/pdf/Maldonado\\_Complaint.pdf](http://www.foxnews.com/projects/pdf/Maldonado_Complaint.pdf)  
Filed Feb 13th, 2007
- "U.S. Citizen Sentenced to Prison for Receiving Military Training from a Terrorist Organization," July 20th, 2007,  
[http://www.usdoj.gov/opa/pr/2007/July/07\\_nsd\\_531.html](http://www.usdoj.gov/opa/pr/2007/July/07_nsd_531.html)

# Offered Without Comment

Ex-Houstonian Arrested and on Trial in USA - Islamic Networking

http://talk.islamicnetwork.com/showthread.php?t=12829

02-14-2007, 07:41 PM #8

**fatimahye**  
Admin  
Join Date: Jan 2005  
Posts: 1,837  
Gender: ♀

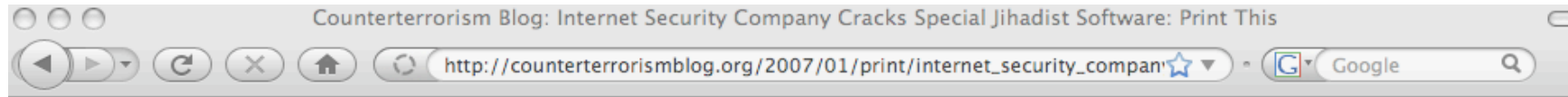
subhanallah,  
we just heard about this today  
and i don't know all the details or facts, but all i can say is  
daniel was an amazing brother who worked for us - he made some really beneficial posts for a while (part of his work to bring benefit to the forums), handled info box, etc. - but was so dedicated to IN - he also updated the news, etc.  
his family was our family and vice versa  
a while back, though, he fell out of touch with us, which didn't alarm us at first since when he first settled he would be out for weeks and then finally get net access etc.

02-14-2007, 07:48 PM #10

**mujaahidah**  
Senior Member  
Join Date: Nov 2006  
Posts: 937

Subhanallah!  
Is it just me, or is every mod and person associated with the forum bein arrested???  
I've bookmarked LOADS of this brother's posts on books and his recommendations!

# Another Example: "Mujahedine Secrets"



## Internet Security Company Cracks Special Jihadist Software

By Andrew Cochran

CT Blog posting from Jim Melnick, iDefense Intelligence Team, VeriSign, Inc.

On January 1, 2007, the pro-terrorist group, "Global Islamic Media Front" (GIMF) announced the "imminent release" of what they called "the first Islamic computer program for secure exchange on the Internet." Some Western websites that track online terrorist activity reported on the GIMF announcement, but it has otherwise not received any serious media attention. iDefense/VeriSign has since found a copy of this program, "Mujahedine Secrets," on a pro-terrorist Arabic language forum and has begun analyzing its capabilities and assessing what its impact will be. Earlier this week we announced this to our client base, which includes numerous key elements of the U.S. government. We are continuing to discover new aspects about the software, which we believe is bound to spread quickly in the online pro-terrorist world. As far as is known, none of this new information has been announced publicly anywhere else other than among the pro-terrorists themselves.

The "Mujahedine Secrets" encryption program offers terrorists and their sympathizers several key features, some of which are common features of PGP programs that are currently available elsewhere as well as other features that appear to be new. Technical analysis is ongoing and will be assessed in future iDefense reporting. Most importantly, this program is an executable application that does not need to be installed onto a PC and can be used with a USB drive. According to iDefense Middle East analyst Andretta Summerville, "the program's 'portability' as an application (not requiring installation) will become an increasingly desirable feature, especially considering the high use of Internet cafés worldwide by pro-terrorist Islamic extremists." The use of the 'Mujahedine Secrets' on a portable USB drive will offer additional anonymity to those who use the program, which may make it increasingly difficult or even impossible for investigators to track down the source of activity further than the Internet café itself.

## Mujahideen Secrets 2

Mujahideen Secrets 2 is a new version of an encryption tool, ostensibly written to help Al Qaeda members encrypt secrets as they communicate on the Internet.

[A bunch of sites have covered this story](#), and a couple of security researchers are quoted in the various articles. But quotes like [this](#) make you wonder if they have any idea what they're talking about:

Mujahideen Secrets 2 is a very compelling piece of software, from an encryption perspective, according to Henry. He said the new tool is easy to use and provides 2,048-bit encryption, an improvement over the 256-bit AES encryption supported in the original version.

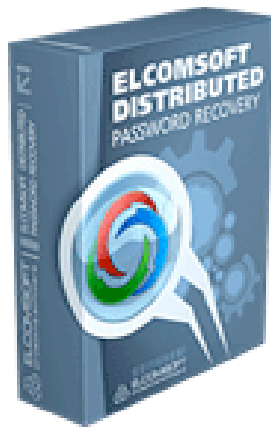
No one has explained why a terrorist would use this instead of [PGP](#) -- perhaps they simply don't trust anything coming from a U.S. company. But honestly, this isn't a big deal at all: strong encryption software has been around for over fifteen years now, either cheap or free. And the NSA probably breaks most of the stuff by [guessing the password](#), anyway. Unless the whole program is an NSA plant, that is.

My question: the articles claim that the program uses several encryption algorithms, including RSA and AES. Does it use Blowfish or Twofish?

[Posted on February 8, 2008 at 5:39 AM](#) • [55 Comments](#) • [View Blog Reactions](#)



## Elcomsoft Distributed Password Recovery



### High-Performance Distributed Password Recovery

Break complex passwords, recover strong encryption keys and unlock documents in a production environment. Elcomsoft Distributed Password Recovery is a high-end solution for forensic and government agencies, data recovery and password recovery services and corporate users with multiple networked workstations connected over a LAN or the Internet. Featuring unique acceleration technologies and providing linear scalability with no overhead, Elcomsoft Distributed Password Recovery offers the fastest password recovery by a huge margin, and is the most technologically advanced password recovery product currently available.

### Features and Benefits

- NVIDIA GPU acceleration (patent pending) reduces password recovery time by a factor of 20
- Linear scalability with no overhead allows using up to 10,000 workstation without performance drop-off
- Broad compatibility recovers document and system passwords to various file formats ([click for the complete list of formats](#))
- Distributed password recovery over LAN, Internet or both
- Console management for flexible control from any networked PC
- Plug-in architecture allows for additional file formats



October 30, 2001

## **Veiled Messages of Terror May Lurk in Cyberspace**

By GINA KOLATA

The investigation of the terrorist attacks on the United States is drawing new attention to a stealthy method of sending messages through the Internet. The method, called steganography, can hide messages in digital photographs or in music files but leave no outward trace that the files were altered.

Intelligence officials have not revealed many details about whether, or how often, terrorists are using steganography. But a former French defense ministry official said that it was used by recently apprehended terrorists who were planning to blow up the United States embassy in Paris.

The terrorists were instructed that all their communications were to be made through pictures posted on the Internet, the defense official said.

The leader of that terrorist plot, Jamal Beghal, told French intelligence officials that he trained in Afghanistan and that before leaving that country for France, he met with an associate of Osama bin Laden. The plan was for a suicide bomber to drive a minivan full of explosives through the embassy gates.

The idea of steganography is to take advantage of the fact that digital files, like photographs or music files, can be slightly altered and still look the same to the human eye or sound the same to the human ear.

The only way to spot such an alteration is with computer programs that can notice statistical deviations from the expected patterns of data in the image or music. Those who are starting to look for such deviations say that their programs are as yet imperfect but that, nonetheless, some are finding widespread use of steganography on the Internet. For national security reasons some of these experts do not want to reveal exactly what they find, and where.

"Quite an alarming number of images appear to have steganography in them," said one expert who has looked for them, Chet Hosmer, the president and chief executive of WetStone Technologies in Cortland, N.Y.

<http://query.nytimes.com/gst/fullpage.html?res=9B01E3D91730F933A05753C1A9679C8B63> 73

# But Note the Conclusion of "Detecting Steganographic Content on the Internet"...

- <http://www.citi.umich.edu/techreports/reports/citi-tr-01-11.pdf>

*At this writing, Crawl has downloaded over two million images from eBay auctions. For these images, Stegdetect indicates that about 17,000 seem to have steganographic content. Of these 17,000 images, 15,000 supposedly have content hidden by JPHide. All 15,000 images have been processed by Stegbreak.*

*While Stegbreak has been running on a cluster of 60 machines, it is still too slow to process all images that Stegdetect finds. We hope that we will have access to more and better machines in the future.*

*To verify the correctness of all participating clients, we insert tracer images into every Stegbreak job. As expected the dictionary attack finds the correct passwords for these images. However, **so far we have not found a single genuine hidden message.** We offer three possible explanations to support our results:*

- There is no significant use of steganography on the Internet.*
- Nobody uses steganographic systems that we can find.*
- All users of steganographic systems carefully choose passwords that are not susceptible to dictionary attacks.*

**IX. “High Tech” War That Isn't  
Computer or Network Focused,  
and the Other End of the Spectrum,  
“Non-Technical” Military  
Information Operations**

# Some Types of “High Tech” Weapons Simply Aren’t Primarily Computer or Network Oriented

- There’s a (wrong headed) temptation to lump **any** sort of “high tech” warfare or weapon into the “cyber” category. Please don’t. If an attack or a weapon isn’t directly tied to computers or networks, it may be a weapon or an attack, but it *isn’t* a “cyber war” method or weapon.
- Examples of stuff that we’ll arbitrarily put **out of scope** includes:
  - **satellite-related stuff** (such as satellite guided munitions), except for satellite services relating to IP (or other data) networks
  - **radio frequency stuff** (such as jamming and “electronic warfare”), except for WiFi and related wireless IP networking
  - **lasers and other sorts of “beam” or directed energy weapons**
  - **less than lethal weapons** (sonic, thermal, or foam weapons, etc.)
  - potential **nanotechnology weapons** and other exotic stuff.
- Let’s also unilaterally exclude embedded battlefield weapon system computers, and things like unmanned aerial drones, battlefield sensor networks, and other tactical intelligence collection systems

# The Sort of ‘Network War’ I’m Not Interested In

*[...] no one had ever crystallized what the information age might offer the Pentagon quite like Cebrowski and Garstka did. In an article for the January 1998 issue of the naval journal Proceedings, "**Network-Centric Warfare: Its Origin and Future**," they not only named the philosophy but laid out a new direction for how the US would think about war.*

*[...] “Nations make war the same way they make wealth,” Cebrowski and Garstka wrote. Computer networks and the efficient flow of information would turn America's chain saw of a war machine into a scalpel.*

*The US military could use battlefield sensors to swiftly identify targets and bomb them. Tens of thousands of warfighters would act as a single, self-aware, coordinated organism. Better communications would let troops act swiftly and with accurate intelligence, skirting creaky hierarchies. It'd be "a revolution in military affairs unlike any seen since the Napoleonic Age," they wrote. And it wouldn't take hundreds of thousands of troops to get a job done — that kind of "massing of forces" would be replaced by information management. "For nearly 200 years, the tools and tactics of how we fight have evolved," the pair wrote. "Now, fundamental changes are affecting the very character of war.”*

[http://www.wired.com/print/politics/security/magazine/15-12/ff\\_futurewar](http://www.wired.com/print/politics/security/magazine/15-12/ff_futurewar)<sub>77</sub>  
[emphasis added]

# NON-Technical Military Information Operations

- At the other end of the spectrum, I also want to exclude “non-technical” military “information operations” -- the sort of stuff that’s sometimes known as “influence operations” or “psychological operations” or “military deception operations.”
- All of those are important, and all of them make valuable contributions to our war fighting capabilities, they just don’t fit what I’m defining to be “cyber war.”
- I will say that I do recognize that modern military information operations have come a long way beyond just running sound trucks and dropping leaflets from airplanes, although 30,000,000 leaflets were dropped during the Gulf War (see the following slide for an example).
- As an example of how psychological operations have moved beyond just sound trucks and leaflet drops, note the comment “There were American special operations forces and CIA operatives making *speed-dial cell phone calls to the numbers of some Iraqi generals*, trying to rattle them, make them think that war was imminent -- which it was -- try to persuade them not to fight.”  
[www.pbs.org/wgbh/pages/frontline/shows/invasion/interviews/purdum.html](http://www.pbs.org/wgbh/pages/frontline/shows/invasion/interviews/purdum.html)
- I’d also note the National Guard’s recently created “Warrior” video, featuring Kid Rock and Dale Earnhardt, Jr., a masterful effort to recruit soldiers from the “YouTube” generation. It is being screened in theaters prior to feature films, and shown online via YouTube and <http://www.nationalguardwarrior.com/><sup>78</sup>



## Surrender Passes

At the same time the US Airforce began using its planes and helicopters to shower enemy military groupments in Kuwait and Iraq with a variety of surrender passes. Up to four millions of these had been disseminated towards the end of January and a few days later some fourteen millions of all types had been disseminated from a variety of American aircraft. In all, almost 30 million leaflets of all kinds are now officially said to have been printed and eventually disseminated during the short war.



Facsimile 25-dinar banknote



# Example of Some “Information Operations” Related Topics at Air University

"Air Education and Training Command - Develop America's Airmen Today...For Tomorrow"

## AIR UNIVERSITY

THE INTELLECTUAL AND LEADERSHIP CENTER OF THE AIR FORCE  
We make a difference, one student at a time.

### Cyberspace & Information Operations Study Center

*Mens agitat molem - Virgil*  
(Mind moves matter)

[AWC Gateway to Internet](#) | [Air University Library](#) | [military portal](#)  
other centers - [strategy & technology](#) | [space](#) | [culture](#) | [terrorism](#)

### Cyberspace and Information Operations Symposium, July 15-17, 2008

[What Are Info-Ops About This Center](#)

[Cyberspace](#)  
[Network Warfare Ops](#)  
[Electronic Warfare](#)

[Influence Ops](#)

- o [Psychological Operations](#)
- o [Military Deception](#)
- o [Operations Security](#)
- o [Counterpropaganda](#)
- o [Counterintelligence](#) \*\*
- o [Public Affairs](#) \*\*

[General Info](#)  
[Organizations](#)  
[Law & Policy](#)  
[US Doctrine](#)  
[International](#)  
[Infowar, Information Warfare](#)  
[Perception](#)  
[Laboratories](#)



[Strategic Communication](#)  
[IO - USGOV, Nonmil](#)  
[IO - Joint & Services](#)  
[IO - USAF](#)

[Education](#)  
[Research & Theory](#)  
[Reference](#)  
[Related Topics](#)  
blogs, fiction, etc.  
[Links](#)

[Index, by Subject](#)

see also  
[Media-Public Affairs](#) \*\*  
[Public Diplomacy](#) \*\*  
[Intelligence](#) \*\*  
[Lessons Learned](#) \*\*  
[Net Centric Warfare](#) \*\*  
[Communication Skills](#) \*\*  
[Thinking Skills](#) \*\*

\*\* located on the  
[AWC Gateway to the Internet](#)



**X. So Is There ANYTHING That Really  
"Counts" as "Cyber War?"**

**YES!**

# **Let's Consider Five Examples of Attacks That I DO Consider to Be Illustrative of Real Cyber War**

1. Low-intensity persistent asymmetric economic cyber attacks, such as spam
2. Cyber attacks on fundamental Internet protocols such as DNS (the domain name system) or BGP (the Internet's wide area routing protocols)
3. Kinetic ("physical") attacks on high value Internet “choke points” such as cable landing sites or Internet exchange points
4. Operations conducted against critical civilian infrastructure such as industrial control systems (so-called “SCADA” systems)
5. Strategic high altitude strikes aimed at destroying or disrupting national infrastructure on a wide-scale through electromagnetic pulse (EMP) effects

Let's start by looking at spam.

## **X. Low Intensity, Asymmetric, Persistent, Economic Attacks, Such As Spam**

# “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?



# SENDERBASE® IRONPORT SECURITY NETWORK

[Blocked?](#) | [Subscribe](#) | [Contact](#)

Enter domain, network owner,  
IP address or CIDR range **[?]**

[HOME](#)

[SENDERBASE QUERIES](#)

[THREAT OPERATIONS CENTER](#)

[SPAMCOP](#)

[ABOUT](#)

## HOME

### Summary Reports

- + Current Threats
- + Spam Watch
- + Virus Watch

### Email & Web Reputation

- + Look Up

### Detailed Reports

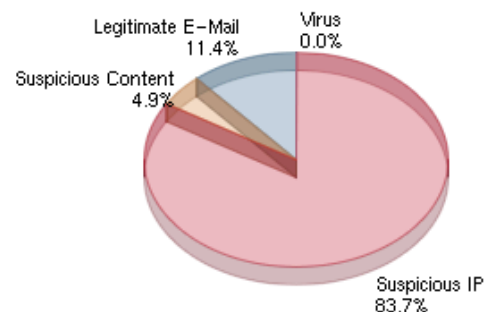
- + Global Email Traffic
- + Spam Traffic
- + Virus Traffic
- + Threat Activity Locator



### SPAM ACTIVITY SOURCE

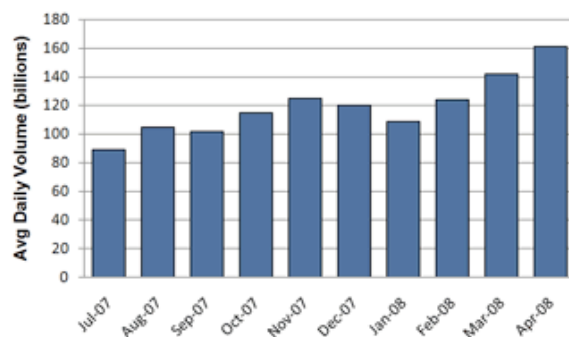


### EMAIL THREAT TYPE

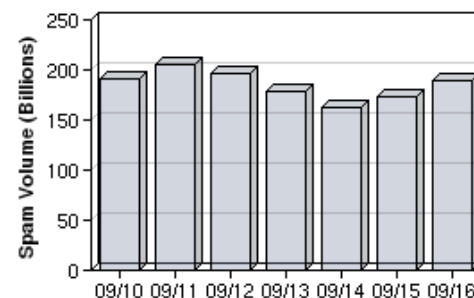


**<== 11.4%  
Legitimate  
Email**

### GLOBAL SPAM (MONTHLY)



### GLOBAL SPAM (LAST 7 DAYS)



**<== 200  
BILLION  
Spam/day**

# 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) <sup>86</sup>

# 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."  
<http://www.newswiretoday.com/news/32531/>

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:

$\$42,000,000,000 / 301,139,947 \text{ people} / 365 \text{ days per year} =$   
"just" \$0.382 per American per day, or \$11.46/American/month

## For Comparison, Some Other Recent Costs

- "Hurricane Katrina cost insurers an inflation-adjusted \$43 billion," [http://money.cnn.com/2008/09/13/news/economy/ike\\_effect/](http://money.cnn.com/2008/09/13/news/economy/ike_effect/)
- "The attack on the World Trade Center will cost New York City \$83 billion to \$95 billion," <http://query.nytimes.com/gst/fullpage.html?res=940DE3DF143EF936A3575AC0A9649C8B63>
- "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...

- Consider John Robb's 15 Aug 2008 posting "Open Source Warfare: Cyberwar," ( <http://globalguerrillas.typepad.com/globalguerrillas/2008/08/open-source-war.html> ):

*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?
- A positive note: “Congress Passes Ryan Haight Online Pharmacy Consumer Protection Act,” October 1st, 2008, see <http://www.usdoj.gov/dea/pubs/pressrel/pr100108.html>

# **XI. Cyber Attacks On Fundamental Internet Protocols Such as DNS or BGP**

# “National Strategy To Secure Cyberspace”

- “1. Secure the Mechanisms of the Internet”

“a. Improve the Security and Resilience of Key Internet Protocols

“Essential to the security of the Internet infrastructure is ensuring the reliability and secure use of three key protocols:

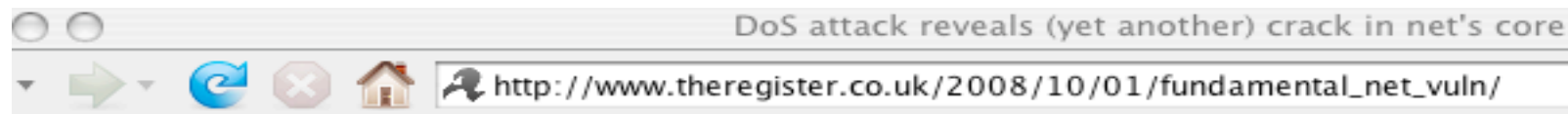
the Internet Protocol (IP),  
the Domain Name System (DNS), and  
the Border Gateway Protocol (BGP).”

*Source:*

[http://www.whitehouse.gov/pcipb/cyberspace\\_strategy.pdf](http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf)

pp. 30 (source document page numbering)

[PCIPB=“President’s Critical Infrastructure Protection Board”]<sub>92</sub>



Security experts say they have discovered a flaw in a core internet protocol that can be exploited to disrupt just about any device with a broadband connection, a finding that could have profound consequences for millions of people who depend on websites, mail servers, and network infrastructure.

The bug in the transmission control protocol (TCP) affords attackers a wealth of new ways to carry out denials of service on equipment at the heart of data centers and other sensitive points on the internet. The new class of attack is especially severe because it can be carried out using very little bandwidth and has the ability to paralyze a server or router even after the flood of malicious data has stopped.

"If you use the internet and you serve a TCP-based service that you value the availability for, then this affects you," Robert E. Lee, chief security officer for Sweden-based Outpost24 told *The Register*. "That may not be every internet user, but that's certainly any IT manager, that's certainly any website operator, mail server operator, or router operator."

Lee said he and Outpost24 colleague Jack Louis discovered the bug in 2005, but decided to keep their finding secret while they tried to devise a solution. After largely hitting a wall, they decided to go public in hopes that a new infusion of ideas will finally get the problem fixed.

Other security experts have already weighed in on the TCP bug and said it appears Outpost24 isn't overstating its severity. Robert "RSnake" Hansen, who has been briefed by Lee, told *El Reg* it's "the most serious thing I've heard of in a month or two."

Robert Graham, CEO of Errata Security, [said here](#) that after listening to [this interview](#) with the researchers, he's inclined to believe the threat is real.

# “What About IPv6?” Deployment of IPv6 Will NOT Materially Improve Our Network Security

- While we do need rapid deployment of IPv6, that requirement is driven by the rate of IPv4 address exhaustion, **not** by security-related considerations.  
See <http://www.potaroo.net/tools/ipv4/index.html>  
*Trivia quiz: do folks know when we're likely to run out of IPv4 addresses?\**
- IPv6 has many of the same vulnerabilities that IPv4 does, and a site with IPv4 and IPv6 may see both improvements and some new problems when it comes to their site's overall security. For example, because IPv6 address blocks tend to be large, they make it more difficult for an adversary to attempt to exhaustively map IPv6 address ranges. On the other hand, just to mention one factor, many security appliances have limited support for IPv6, which means that IPv6 traffic may be largely opaque to security staff monitoring.

See “IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0),”  
[http://www.cisco.com/security\\_services/ciag/documents/v6-v4-threats.pdf](http://www.cisco.com/security_services/ciag/documents/v6-v4-threats.pdf)

-----

\* As of 2-Oct-2008, the best estimates are 18 Nov 2010 (at IANA),  
and 18 Nov 2011 (at the RIRs), but those dates may/will change over time<sub>94</sub>

# How Much IPv6 Deployment Has Taken Place So Far? “*Not Much*”

http://asert.arbornetworks.com/2008/8/the-end-is-near-but-is-ipv6/



Google

You can view the full technical report at  
<http://www.arbornetworks.com/IPv6research>.

## What did we find?

Not much. In fact, less than not much — very, very little.

The below shows the percentage of IPv6, both native and tunneled, as a percentage of all Internet traffic. At its peak, IPv6 represented less than one hundredth of 1% of Internet traffic. This is somewhat equivalent to the allowed parts of contaminants in [drinking water](#) (my household water comes from the Detroit river).

The “good news?” We still have “lots” of time <cough!> to get rolling with IPv6 -- remember, we won’t run out of IPv4 addresses for ~ 3 years. That’s, um, still “*plenty*” of time (NOT!)

# Securing The Domain Name System

- I have addressed/will address the security of the domain name system in a separate talk while here in North Dakota, so I'm not going to talk about that topic here during this session.

- To see that DNSSEC talk, go to

<http://www.uoregon.edu/~joe/dnssec-nd/>

- I will repeat for the record, however, that DNSSEC has had a glacially slow roll out to-date.



# Securing Wide Area Routing

- The routing of network traffic across the Internet is controlled by a protocol known as "BGP."
- BGP in its current form is vulnerable to a variety of attacks, attacks which can have profound effects on even the biggest sites.
- Alexa ranks the top three global web sites as:
  1. Google
  2. Yahoo
  3. YouTube

Due to an unintentional BGP misconfiguration, a Pakistani ISP accidentally diverted all traffic meant for Youtube, the #3 Internet site worldwide, to the Pakistani ISP's network (thereby crushing itself, but also interfering with access to Youtube for everyone else).

- While this was an unintentional incident, one could easily imagine a cyber enemy intentionally mounting similar attacks.

# "Pakistan Move Knocked Out YouTube"

(CNN) -- An apparent move by the Pakistani government to block YouTube, the popular video-sharing Web site, knocked out access to the site worldwide for more than two hours, Internet analysts say.

The outage followed a letter sent Friday evening by the Pakistani Telecommunications Authority (PTA) to Internet service providers, ordering them to prevent people in Pakistan from visiting YouTube.

The authority cited a "highly blasphemous" video featuring right-wing Dutch politician Geert Wilders.

The block was intended to cover only Pakistan but extended to about two-thirds of the global Internet population, The Associated Press cited Renesys Corp, an Internet monitoring company, as saying.

What happened was that Pakistan Telecom established a route that directed requests for YouTube videos from local Internet subscribers to a "black hole," AP cited Renesys as saying. It then published that route to its international data carrier, PCCW of Hong Kong, which accepted, AP quoted Todd Underwood, vice president of Renesys, as explaining.

The move also coincided with the temporary shutdown Friday evening of Aaj TV, a Pakistani television cable and satellite channel, after it reportedly upset President Pervez Musharraf. Since declaring a nationwide state of emergency on November 3, he has taken independent television stations off the air; they would later be allowed to resume service.

In YouTube's case, it was completely inaccessible on Sunday from 10:48 a.m. PT to 12:51 p.m. PT (11:48 p.m. Sunday to 1:51 a.m. Monday in Pakistan), said Shawn White, a spokesman for Keynote Systems, a San Mateo, California-based Internet-performance monitoring company.

Keynote Systems' monitoring of major Web sites like YouTube includes attempting to access them every 15 minutes from computers in 35 cities in Europe, Asia and the Americas, White said.

"I was kind of surprised that something like this could happen, especially globally," said White, calling the outage the most high-profile Internet blackout he remembers in his 12 years with the company. "It just further illustrates just how fragile the Internet can be.

# BGP Attacks Can Also Be Used For Cyber Espionage



Two security researchers have demonstrated a new technique to stealthily intercept internet traffic on a scale previously presumed to be unavailable to anyone outside of intelligence agencies like the National Security Agency.

The tactic exploits the internet routing protocol BGP (Border Gateway Protocol) to let an attacker surreptitiously monitor unencrypted internet traffic anywhere in the world, and even modify it before it reaches its destination.

The demonstration is only the latest attack to highlight fundamental security weaknesses in some of the internet's core protocols. Those protocols were largely developed in the 1970s with the assumption that every node on the then-nascent network would be trustworthy. The world was reminded of the quaintness of that assumption in July, when researcher [Dan Kaminsky disclosed](#) a serious vulnerability in the DNS system. Experts say the new demonstration targets a potentially larger weakness.

"It's a huge issue. It's at least as big an issue as the DNS issue, if not bigger," said Peiter "Mudge" Zatkos, noted computer security expert and former member of the L0pht hacking group, who testified to Congress in 1998 that he could bring down the internet in 30 minutes using a similar BGP attack, and disclosed privately to government agents how BGP could also be exploited to eavesdrop. "I went around screaming my head about this about ten or twelve years ago.... We described this to intelligence agencies and to the National Security Council, in detail."

# Learning More About The BGP Vulnerabilities

## ... And How We Might Be Able To Fix It

- I've got an entire talk discussing routing vulnerabilities, so if you're interested in learning more about that issue check out "Route Injection and the Backtrackability of Cyber Misbehavior," <http://www.uoregon.edu/~joe/fall2006mm/fall2006mm.pdf>
- A nice overview of how we might be able to begin to secure BGP can be found in, "Securing BGP Through Secure Origin BGP," [http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ipj\\_6-3/securing\\_bgp\\_sobgp.html](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/securing_bgp_sobgp.html)
- Another approach to potentially securing BGP can be found at <http://www.ir.bbn.com/sbgp/>
- Comparing them: <http://www.nanog.org/mtg-0306/pdf/meyer.pdf> , [http://www.cs.cmu.edu/~dwendlan/routing/SoBGP\\_SBGp.ppt](http://www.cs.cmu.edu/~dwendlan/routing/SoBGP_SBGp.ppt)
- To date, however, work on securing BGP has been very, very slow (even slower than the IPv6 or DNSSEC rollouts!)

## **XII. Kinetic Attacks On High Value Internet “Choke Points”**

# Cyberwar As Destructive Physical (“Kinetic”) Attacks Upon Key Internet Infrastructure Itself

- The Internet has been architected to detect failures and usually route around them, but that’s not always possible.
- At least in some cases, accidents or intentional, coordinated, and **physically destructive** acts have the potential to cause noticeable operational damage to the Internet.
- Such kinetic attacks would likely target “Internet choke points:”
  - carrier hotels where providers meet to exchange network traffic
  - trans-oceanic circuits (for a great tutorial on submarine cables, by the way, see "Mother Earth, Mother Board," <http://www.wired.com/wired/archive/4.12/ffglass.html> ), and
  - route-limiting geographical features such as bridges (over wide rivers or gorges) and tunnels, etc., etc., etc.
- Coordinated intentional attacks by knowledgeable insiders targeting particularly vulnerable sites, or multiple live & backup connections simultaneously, represent particularly dangerous attack scenarios.

# The Exchange Point/Carrier Hotel/Private Network Interconnect (PNI) Vulnerability

*"The most dangerous vulnerability is the aggregation of high-capacity bandwidth circuits into a small number of unprotected carrier hotels in which several hundred network operators interconnect their circuits in one nonsecure building. These buildings often feed directly into the international undersea cable system. Security is often farcical. This lack of protection exists in several carrier hotels on transit points along the axis of the international telecommunications system that includes Dubai, Zurich, Frankfurt, London, New York, San Francisco, Los Angeles, Tokyo, Hong Kong and Singapore. In addition to being the most important channel for military communications today, this also is the telecommunications axis of the international finance system."*

"Cybersecurity Demands Physical Security," [emphasis added]  
[http://www.afcea.org/signal/articles/templates/  
SIGNAL\\_Article\\_Template.asp?articleid=1085&zoneid=175](http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1085&zoneid=175)



March 11, 2007

# Al-Qaeda plot to bring down UK internet

David Leppard

SCOTLAND YARD has uncovered evidence that Al-Qaeda has been plotting to bring down the internet in Britain, causing chaos to business and the London Stock Exchange.

In a series of raids, detectives have recovered computer files revealing that terrorist suspects had targeted a high-security internet "hub" in London.

The facility, in Docklands, houses the channel through which almost every bit of information on the internet passes in or out of Britain.

The suspects, who were arrested, had targeted the headquarters of Telehouse Europe, which houses Europe's biggest "web hotel", containing dozens of "servers", the boxes which contain the information that makes up the web.

Security experts say the plot against Britain's internet "hub" reflects the constantly changing threat from Al-Qaeda and related Islamic extremist groups.

Last year MI5 uncovered intelligence which suggested that Islamic terrorist suspects had carried out reconnaissance of the huge Bacton complex of gas terminals on the Norfolk coast. The threat led to the deployment of armed guards around the plant.

A senior Whitehall security official said the internet plotters appeared to be planning to infiltrate the "hub", possibly to blow it up from the inside, according to evidence on a computer hard drive seized in raids on the homes of terror suspects in southern England last year.

"The Telehouse facility was the subject of intense reconnaissance. The evidence suggests that it was one of a range of options considered by the suspects," the official said.



# Proposition for Your Consideration

- **As very high value assets, Internet carrier hotels/Internet exchange points should be protected at least as well as we protect airports.**
- Risks to those key Internet facilities include improvised explosive devices (IEDs) introduced into the core of the facility (e.g., secreted within computer or network equipment),\* or large vehicle-borne improvised explosive devices (VBIEDs)\*\* parked at/near the facility
- Yet do Internet exchange points consistently screen all equipment brought into the facilities for dangerous materials? Do trained canine explosive detection teams periodically sniff those buildings? Are vehicles prevented from parking in (or near) the facilities? In most cases the answer to all those questions is “no.”
- A notable exception when it comes to exchange point physical security: Netnod-IX in Sweden operates multiple national exchange points that are reportedly particularly carefully hardened.

-----

- \* See, for example: “Data Center Threats and Vulnerabilities,” <http://www.zdziarski.com/papers/Data%20Center%20Vulnerabilities.pdf>
- \*\* See “Vehicle Born Improvised Explosive Device – VBIED: Terrorist Weapon of Choice,” <http://www.blackwaterusa.com/btw2005/articles/vbied.html>

# **Disasters Can Also Expose Vulnerabilities: The Taiwan Earthquake, December 26th, 2006**

- Strong earthquakes (magnitude 6.7-7.1) occurred off Taiwan's southern coast, damaging two of seven sub-oceanic cables
- Taiwan's largest phone company, Chungwa Telecom, reported that with those two cables going down:
  - they lost 60% of their telephone service to the U.S.
  - 98% of Taiwan's connectivity with Malaysia, Singapore, Thailand, and Hong Kong was down

[http://www.washingtonpost.com/wp-dyn/content/article/2006/12/26/AR2006122601217\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2006/12/26/AR2006122601217_pf.html)
- What happened to media diversity, eh? Yes, satellite latencies are a drag, but backup satellite connectivity would be better than nothing when fiber breaks.

# CSX Howard Street Tunnel Fire, Baltimore\*

- A 60 car train derailed and caught fire in the Howard Street Tunnel under Baltimore MD, the afternoon of July 18th 2001. 1.7 miles in length, the Howard Street Tunnel is the “longest active underground train route on the East Coast.”
- That tunnel was also used as a route for fiber optic cables, cables which burned as a result of the train fire.

*Media reports stated that a Silicon Valley company tracking Internet traffic said the train accident caused the worst congestion in cyberspace in the three years that it has monitored such data. The link through Baltimore “is basically the 1-95 of Internet traffic into and out of Washington,” said the Director of Public Services for a company that monitors Internet flow by the hour on its Web site. The accident had almost no impact in some areas, including parts of Baltimore, while certain connections were 10 times slower than normal, such as the ones between Washington, D.C., and San Diego.*

- Note: While this particular choke point may (or may not) have been eliminated, I’m sure that there are other similar critical choke points which remain unremediated, whether those are tunnels, bridges, etc.

-----

- \* TR-140 CSX Tunnel Fire,  
<http://www.usfa.dhs.gov/downloads/pdf/publications/tr-140.pdf>

# **XIII. Industrial Control Systems ( “SCADA” Systems)**

# Industrial Control Systems

- Sometimes we think of computers and networks just in terms of “enterprise” systems; you know, laptops and desktops, mail and web servers, database servers and institutional ERP systems, etc.
- There is actually a whole additional category of absolutely critical “forgotten” computers and networks which run the electrical grid, our petroleum pipelines, chemical plants, etc.
- Those control systems are often known as “Supervisory Control and Data Acquisition” systems, or “SCADA” systems.
- You usually don’t see them, but they do perform critical tasks and interface to tangible things in the physical world like pumps and compressors and valves and sensors and if they were to be successfully attacked, things could really go “haywire.”
- SCADA systems are definitely a target of cyber warfare efforts. Let me just give you one concrete example, from the United States,

# **“The Most Monumental Non-Nuclear Explosion and Fire Ever Seen From Space.”**

- Thomas C. Reed, Ronald Reagan’s Secretary of the Air Force, described in his book At The Abyss (Ballantine, 2004, ISBN 0-89141-821-0) how the United States arranged for the Soviets to receive intentionally flawed *process control software* for use in conjunction with the USSR's natural gas pipelines, pipelines which were to generate critically needed hard currency for the USSR.

Reed stated that "The pipeline software that was to run the pumps, turbines, and valves was programmed to go haywire, after a decent interval, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to pipeline joints and welds."

The result? A three-kiloton blast in a remote area of Siberia in 1982, which, only by some miracle, apparently didn't result in any deaths. (For context, the Halifax Fire Museum lists the massive 1917 Mont Blanc ship explosion in the Halifax Harbor at a force of 2.9 kilotons.)

(but also see [www.themoscowtimes.ru/stories/2004/03/18/014.html](http://www.themoscowtimes.ru/stories/2004/03/18/014.html) )

- **The consequences of even accidental control system failures can be substantial...**

# The \$50 Billion Dollar 9/14/2003 U.S. Blackout

- “Starting around 14:14, FE [FirstEnergy] control room operators lost the alarm function that provided audible and visual indications when a significant piece of equipment changed from an acceptable to problematic status. **Analysis of the alarm problem performed by FE after the blackout suggests that the alarm processor essentially “stalled” while processing an alarm event. With the software unable to complete that alarm event and move to the next one, the alarm processor buffer filled and eventually overflowed.** After 14:14, the FE control computer displays did not receive any further alarms, nor were any alarms being printed or posted on the EMS’s alarm logging facilities.

“FE operators relied heavily on the alarm processor for situational awareness, since they did not have any other large-scale visualization tool such as a dynamic map board. The operators would have been only partially handicapped without the alarm processor, had they known it had failed. However, by not knowing that they were operating without an alarm processor, the operators did not recognize system conditions were changing and were not receptive to information received later from MISO and neighboring systems. **The operators were unaware that in this situation they needed to manually, and more closely, monitor and interpret the SCADA information they were receiving.**”

[ftp://www.nerc.com/pub/sys/all\\_updl/docs/blackout/](ftp://www.nerc.com/pub/sys/all_updl/docs/blackout/)

NERC\_Final\_Blackout\_Report\_07\_13\_04.pdf [emphasis added]

# Electrical Control System Attacks Overseas

## CIA: Hackers to Blame for Power Outages

By TED BRIDIS, Associated Press Writer

Friday, January 18, 2008

(01-18) 12:40 PST WASHINGTON (AP) --

Hackers literally turned out the lights in multiple cities after breaking into electrical utilities and demanding extortion payments before disrupting the power, a senior CIA analyst told utility engineers at a trade conference.

All the break-ins occurred outside the United States, said senior CIA analyst Tom Donahue. The U.S. government believes some of the hackers had inside knowledge to cause the outages. Donahue did not specify what countries were affected, when the outages occurred or how long the outages lasted. He said they happened in "several regions outside the United States."

"In at least one case, the disruption caused a power outage affecting multiple cities," Donahue said in a statement. "We do not know who executed these attacks or why, but all involved intrusions through the Internet."

A CIA spokesman Friday declined to provide additional details.

"The information that could be shared in a public setting was shared," said spokesman George Little. "These comments were simply designed to highlight to the audience the challenges posed by potential cyber intrusions."

Donahue spoke earlier this week at the Process Control Security Summit in New Orleans, a gathering of engineers and security managers for energy and water utilities.



# **If You'd Like To Learn More About Control System Cyber Security Issues**

- Like so many other areas, unfortunately we don't have enough time to talk about control system cyber security in any depth, but I do have yet another talk that you can see for “homework” if you like:

“SCADA Security and Critical Infrastructure,”

<http://www.uoregon.edu/~joe/scadaig/infraguard-scada.pdf>

(77 slides)

While it is a few years old now, it is, unfortunately, still all too applicable for the most part, since only limited progress has been made when it comes to securing American control systems.

# **XIV. Strategic Cyber War: Electromagnetic Pulse (EMP) Attacks**

**"A single unsophisticated nuclear missile detonated at high altitude could produce an EMP attack that damages or destroys electronic systems across the entire continental United States.** Satellites in low earth orbit would also be damaged. Millions of Americans could die from starvation and disease as an indirect consequence of an EMP attack that disrupts the infrastructures for transportation, medical services, food and water. However, the most important finding of the EMP Commission is that this threat can be greatly mitigated at modest cost and in 3-5 years.

**"Responding to the EMP Commission report, The Wall Street Journal editorialized on August 12, 'All we can say is, we hope someone in Washington is paying attention.'"**  
[emphasis added]

Letter from Congressman Roscoe G. Bartlett, Ph.D. (R-MD)  
<http://www.house.gov/hensarling/rsc/doc/Bartlett--EMP.pdf>

# **The Military Clearly “Gets” The EMP Issue**

- “The most devastating sort of cyber attack on the U.S. would involve a decidedly kinetic weapon — a nuclear bomb, detonated high over the Earth. Such an explosion would shut down all but the most “hardened” networks and computers within range; the Pentagon has hardened its most critical structures and weapons systems, such as nuclear-capable B-52 bombers, for such an eventuality.”

“Military needs hackers, StratCom chief says,” October 2nd, 2008  
[www.armytimes.com/news/2008/09/military\\_chilton\\_093008w/](http://www.armytimes.com/news/2008/09/military_chilton_093008w/)

# The Potential Costs of An EMP Attack

*If you had a few or perhaps only one or two nuclear weapons, you probably would want to use them in the fashion which imposes the largest damage expectancy on the United States and its military forces.*

*If you are going to go after the military forces and you only have a few, by far and away the most effective way that you could potentially use it is an EMP laydown. If you were going against the American civilization itself, again, the largest damage you could expect to see by far is that associated with EMP laydown.*

*As I said earlier, a large laydown over the lower 48 States has a damage expectancy which can be reckoned in trillions of dollars. Not 10 trillion, but well above a trillion dollars. So what you get the most bang for your nuclear buck out of, you get it out of most heavily damaging your adversary in either the military sense or the sense of civilian infrastructure. EMP is the attack mode of choice.*

Dr. Lowell Wood, LLNL, Congressional Hearings on the Threat Posed by Electromagnetic Pulse (EMP) to U.S. Military Systems and Civil Infrastructure, July 16, 1997, [www.fas.org/spp/starwars/congress/1997\\_h/has197010\\_1.htm](http://www.fas.org/spp/starwars/congress/1997_h/has197010_1.htm)

# If You'd Like To Learn More About EMP

- We don't have time to go into the electromagnetic pulse risk in depth here today, but if you're willing to self-impose still more homework on yourself, see:

“Planning for Certain High Risk Security Incidents,”

<http://www.uoregon.edu/~joe/highrisk/high-risk.pdf> (123 slides)

- The blue ribbon Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack also has just released its 2008 Critical National Infrastructure Report, which I strongly urge everyone to read. It is available online from

<http://www.empcommission.org/>

## **XV. Conclusion**

## Some Closing Thoughts

- Key point: hang in there. The first time you hear a discussion of cyber warfare, cyber terrorism, and cyber espionage it is all too easy to become overwhelmed. Please don't be. Most day-to-day cyber stuff is still working, and folks are beginning to focus their attention on the vulnerable bits that urgently need attention.
- You now have a better understanding of what cyber war is (and isn't!) than most people, so now when you read about “cyber war this” and “cyber war that,” give those articles a closer look.
- Along the way, I've tried to also highlight some “minor things” that you might want to have on your mental radar, such as exhaustion of the IPv4 address space less than one thousand days from now.
- I've also tried to give you some suggestions for further reading, and I'm always happy to try answer questions which may come up.
- Thanks for the chance to talk today! Are there any questions?