My top 5 Movie + Hacking = Epic Fails

1.FireWall
iPod + fax machine (even if you coded OCR software) = fail!

2.SwordFish
All the positive or negative reinforcements are not going to make it possible to visualize the encryption passphrase even to government systems.

3.Independence Day
Option 1 hardly anyone on Earth is using a Mac so of course it would be able to interface with an alien OS. Option 2 these are vastly superior beings so of course they would use a Mac like OS. (Let the OS flame war begin).

4.Transformers
Let me get this straight access to Cray super computers and geniuses from around the country Epic Fail. Take it to a guy with a laptop and in between a game of dance dance revolution alien stream deciphered. I thought the talking truck more plausible.

5.The Net
I know she played a hacker but not even Neo was leet enough to be able to telnet to an email address and connect no less.

“I am walking through a city made of glass and I have a bag full of rocks”

(Dispelling the myths and discussing the facts of Global Cyber-Warfare)

HACKERS CAN TURN YOUR HOME COMPUTER INTO A BOMB

. . . & blow your family to smithereens!

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent “break-ins” that paralyzed the Amazon.com, Buy.com and eBAY websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we've only seen the tip of the iceberg.

“The criminals who knocked out those three major online businesses are the least of our worries,” Yabenson told *Weekly World News*.

“There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can't even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

“It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade.

“As shocking as this is, it shouldn't surprise anyone. It's just the next step in an ever-escalating progression of horrors conceived and instituted by hackers.”

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U. S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an 87-digit Russian security code that would have sent deadly missiles hurtling toward five of America's major cities.

“As dangerous as this technology is right now, it's going to get much scarier,” Yabenson said.

“Soon it will be sold to terrorists cults and fanatical religious-fringe groups.

“Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

“And worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

“That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn't like your looks, can kill you and never be found out.”

Sickos can wreak death and destruction from thousands of miles away!

Arnold Yabenson.

KABOOM! It might not look like it, but an innocent home computer like this one can be turned into a deadly weapon.

guardian.co.uk

News | Sport | Comment | Culture | Business | Money | Life & style | Tr

News › Technology › Internet

Terrorists could use internet to launch nuclear attack: report

The risk of cyber-terrorism escalating to a nuclear strike is growing daily, according to a study

Bobbie Johnson
guardian.co.uk, Friday 24 July 2009 13.01 BST
Article history

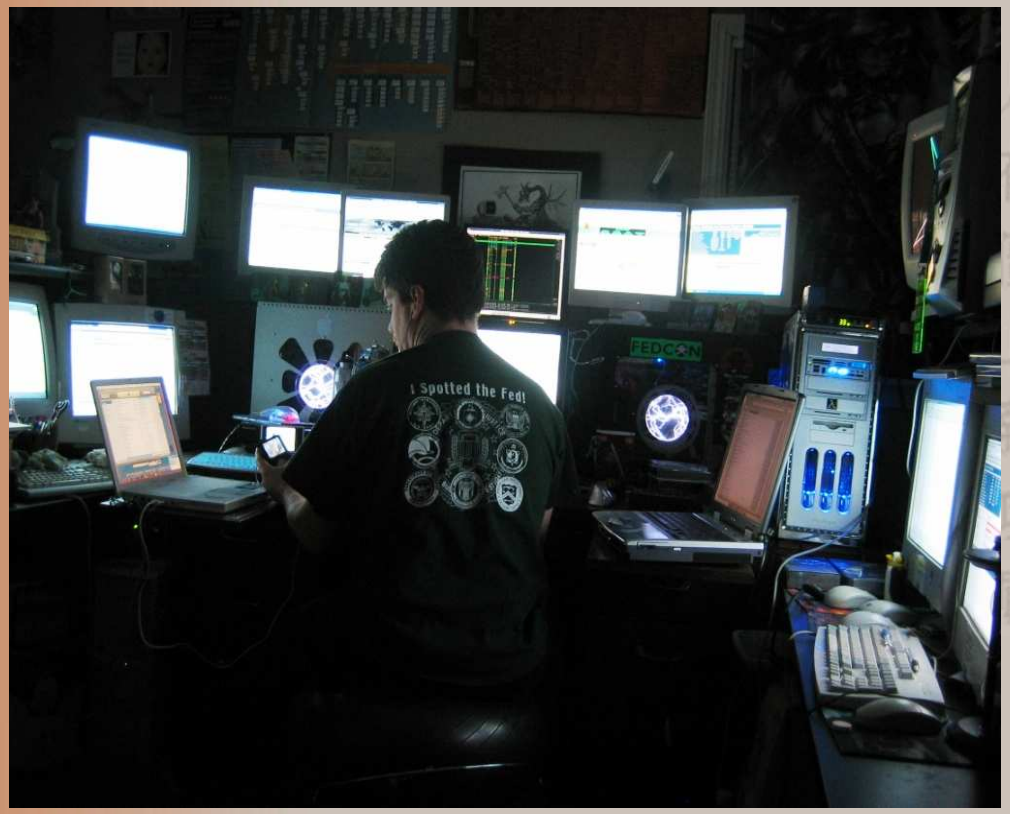
Photograph: U.S. Department of Energy-Nevada/Corbis

Jayson E. Street, CISSP, C|EH,
GSEC, GCIH, GCFA,
IEM, IAM, ETC…

STRATAGEM 1 SOLUTIONS
"DEFENSE THROUGH DISCOVERY"

Let go of my EGO

- Lets start out with a little about yours truly.

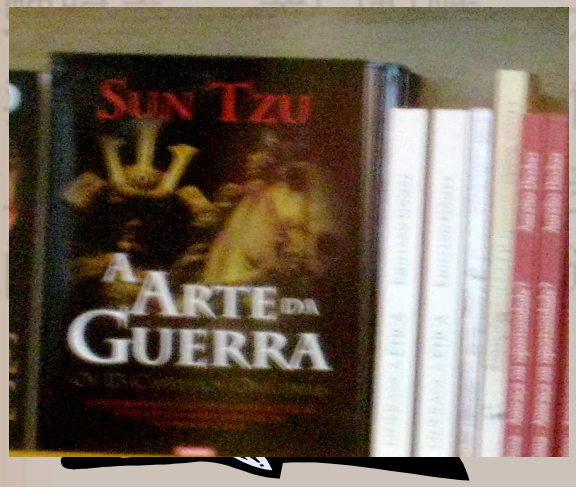


- BRUCON09@F0rb1dd3n.com
http://F0rb1dd3n.com

STRATAGEM 1 SOLUTIONS
"DEFENSE THROUGH DISCOVERY"

Yes Sun Tzu was a hacker!

- Sun Wu (Tzu) “Ping-fa”(The Art of War)
- “Thus it is said that one who knows the enemy and knows himself will not be endangered in a hundred engagements. One who does not know the enemy but knows himself will sometimes be victorious, sometimes meet with defeat. One who knows neither the enemy nor himself will invariably be defeated in every engagement!”



Contents

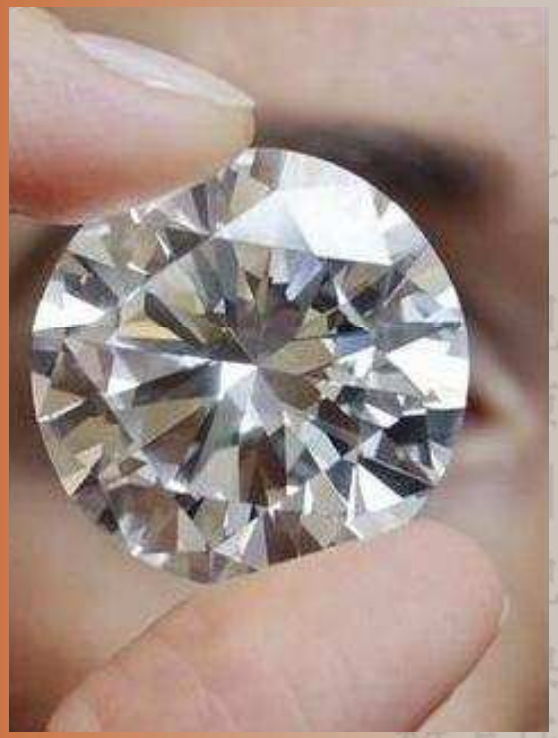
- INTRO
- Caveats
- History & Geography lessons
- Players and Haters
- You’re involved? YES!!
- Discussion

I read it on the Internets

VS.

Report VS. Investigate

Facets of Perspective



VS.

Meet your new neighbors (and they hate you)

- This war is not dictated by boundaries just bandwidth.

- War is God's way of teaching Americans geography.

Ambrose Bierce

The Roster for the B1G Game

- China
- Russia
- Jihadist
- More players
- USA (and friends)

CHINA
(The Axel Witsel of cyber-war)

- **Definition of Red Hacker Alliance:**

- **“A Chinese nationalist hacker network, made up of many independent web sites directly linked to one another in which individual sites educate their members on computer attack and intrusion techniques. “**

It’s a culture thing

In the year 6521

- *60 + 50 + 20 + 10 = LAY LOW! For now ;-)*

- *China not this* *But* *This!*

They started without us

- 1997 Formation of the Green Army Founded by GoodWell (China)
- 1998 Anti-Chinese riots in Indonesia provide the catalyst for the creation of the Red Hacker Alliance.
- 2000 *Honker Union of China founded by Lion / China Eagle Union founded by Wan Tao / Javaphile founded by Coolswallow and Blhuang*
- *2001* Sino-US cyber conflict *1000 web defacement protesting death of Chinese pilot.*

Locked and Loaded

- From Hacker to 黑客

- A picture may be worth a thousand words!
- But the native language is worth ten thousand computers!
- And EIP = 0x41414141 is universal!!

Citizen S0ld13r

- These two things are equal

It’s all about the Mao’s (yuan) baby!

From Russia with ….

Russia's cyber capabilities.

- Russia's 5th-Dimension Cyber Army:
- Military Budget: $40 Billion USD
- Global Rating in Cyber Capabilities: Tied at Number 4
- Cyber Warfare Budget: $127 Million USD Offensive Cyber Capabilities: 4.1 (1 = Low 5 = Significant)

As of May 27, 2008

From Russia with …(cont.)

Cyber Weapons Arsenal in Order of Threat:

- Large, advanced BotNet for DDoS and espionage
- Electromagnetic pulse weapons (non-nuclear)
- Advanced dynamic exploitation capabilities
- Wireless data communications jammers
- Cyber Logic Bombs Computer viruses and worms

- Cyber Weapons Capabilities Rating: Advanced
- Cyber force Size: 7,300 +
- Reserves and Militia: None
- Broadband Connections: 23.8 Million +

As of May 27, 2008

Russia VS. Estonia

(This is a cyber-war talk after all)

Lest we forget

27/04/2007

Russia VS. Georgia

(Military precision or an excuse for poor infrastructure?)

From the telegraph to the T1 it really is all about the information flow!

Russia VS. ????

- “From this information, one can only conclude that Russia has advanced capabilities and the intent and technological capabilities necessary to carry out a cyber attack anywhere in the world at any time.”

- Got Gas?
  (speaker note wait for snickers to die down then proceed)

- Kids or KGB The same still holds true don’t mess with Russia.

Know your enemy
(it is ignorance and fear)

- “ISLAM In Arabic, the word means "surrender" or "submission" to the will of God. Most Westerners think of Islam as one of the two…”
- http://slate.msn.com/id/1008347/

- “When the angels said, 'O Mary, ALLAH gives thee glad tidings of a son through a word from HIM; his name shall be the Messiah, Jesus, son of Mary, honoured in this world and in the next, and of those who are granted nearness to God;”

-- Qur'an, Surah 3:38-48

When Jihad becomes J1H4D

- “The funny thing is that so many of the real Al Qaeda websites are hosted in the US,” he says. “One simple reason is it’s one of the cheaper places to host. They circulate via mailing lists and these sort of out of bounds methods where they can be found. They’re all in Arabic. Not many westerners know Arabic, and everything’s fine until some journalist figures out where the website is.”

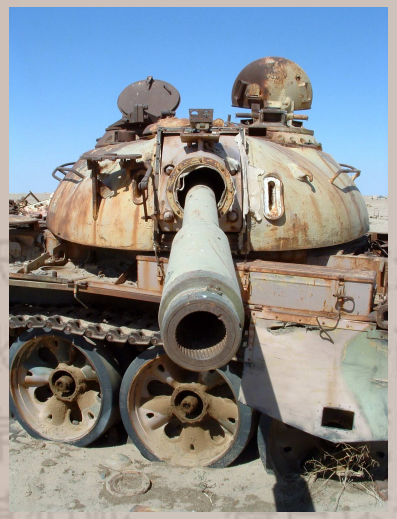
You can’t google for new recruits. (Or can you?)

. “The teams, and the lone gunmen cyber jihadists in this post are : Osama Bin Laden's Hacking Crew, Ansar AL-Jihad Hackers Team, HaCKErS aLAnSaR, The Designer - Islamic HaCKEr and Alansar Fantom. None of these are known to have any kind of direct relationships with terrorist groups, therefore they should be considered as terrorist sympathizers.”

From Brazil to Romania. (and all the trouble in between)

- South America = Community based Hacking
- Eastern Europe = A mix between the movies “Hackers” and “Good Fellas”
- Crime does not = Warfare (usually)

U. S. of OMGWTFBBQ



This > Than = WTF!!!!

Titan rain was the US real wake up call if the NIPRNet can breached what about the SIPRNet? Is the "Trusted Guard" the only thing to stand in the way (hope not) ;-)

STRATAGEM 1 SOLUTIONS
"DEFENSE THROUGH DISCOVERY"

A variation on St4lKing H0rs3

The Non-North Korean DDOS

“A Stalking horse is a person who tests a concept with someone or mounts a challenge against them on behalf of an anonymous third party. If the idea proves viable and/or popular, the anonymous figure can then declare their interest and advance the concept with little risk of failure. If the concept is 'shot down in flames', the anonymous party will not be 'tainted by association' and can either drop the idea completely or 'bide their time' and wait until a better moment for launching an attack.”

All the cool kids are doing it!

From UK’s White hall to Israel’s Shin Bet (yeah I said Israel), ETC…

We must not only learn but adapt!

- *"The smallest detail, taken from an actual incident in war, is more instructive for me, a soldier, than all the Theirs, and Jominis in the world. They speak, no doubt, for the heads of states and armies but they never show me what I wish to know – a battalion, a company, a squad, in action." -Col. Charles Ardant du Picq*
- Battle Studies: Ancient and Modern Battle from Russel A. Gugeler, Combat Actions in Korea, *US Government Printing Office, 1970 revised edition, p. iii*

Okay now what can we do?

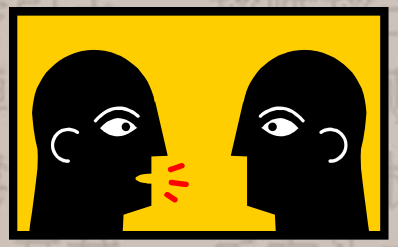
- Without understanding where the opponent's weaknesses are you cannot borrow their strength to use against them. (Cheng Man Ching)

- **http://www.thedarkvisitor.com/**
  (full on props to @HeikeTDV & @jumper_TDV)

- http://stratagem-one.com
- http://netragard.com
- http://www.security-twits.com/
- http://osvdb.org
- http://isc.sans.org
-

Now let's learn from others

- Discussion and Questions????
- Or several minutes of uncomfortable silence it's your choice.



- This concludes my presentation Thank You

The Links

- No order here they are.

- http://ddanchev.blogspot.com/2007/10/russian-business-network.html
- http://www.defensetech.org/archives/004200.html
- http://dsonline.computer.org
- http://www.time.com/time/magazine/article/0,9171,1101040809-674777,00.html
- http://news.cnet.com/8301-1009_3-10049008-83.html
- http://www.thedarkvisitor.com/

- I am sure I missed some though not on purpose. If you do not find a proper source in this list but mentioned in the presentation please contact me and I will correct it.

All those other links in no order

- http://intelfusion.net/wordpress/?p=432
- http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=Storage+Security&articleId=9134010&taxonomyId=153&pageNumber=2
- http://bostonreview.net/BR34.4/morozov.php
- http://www.csoonline.com/article/495520/Cyberwar_Is_Offense_the_New_Defense_
- http://www.itar-tass.com/eng/level2.html?NewsID=14070168&PageNum=0
- http://www.google.com/hostednews/afp/article/ALeqM5geMDsdejQoeSn8FQseQHZKeTe50A
- www.heritage.org/research/asiaandthepacific/upload/wm_1735.pdf
- http://www.nap.edu/nap-cgi/report.cgi?record_id=12651&type=pdfxsum
- http://news.bbc.co.uk/2/hi/uk_news/politics/8118729.stm
- http://en.wikipedia.org/wiki/Honker_Union
- http://blog.security4all.be/
- http://www.nytimes.com/2009/04/28/us/28cyber.html?_r=2
- http://www.nytimes.com/2009/03/29/technology/29spy.html?_r=3&hp
- http://www.foxnews.com/story/0,2933,464264,00.html?sPage=fnc/scitech/cybersecurity
- http://www.foxnews.com/story/0,2933,448626,00.html?sPage=fnc/scitech/cybersecurity
- http://www.foxnews.com/story/0,2933,403161,00.html?sPage=fnc/scitech/cybersecurity
- http://www.foxnews.com/story/0,2933,370243,00.html?sPage=fnc/scitech/cybersecurity
- http://www.spiegel.de/international/germany/0,1518,606987,00.html
- http://threatchaos.com/
- http://www.popsci.com/scitech/article/2009-04/hackers-china-syndrome
- http://shanghaiist.com/2009/06/08/how_to_make_money_as_a_hacker.php

All those other links (cont.)

- http://www.socialsignal.com/blog/rob-cottingham/censorship-isnt-only-problem-with-chinas-new-internet-blocking-software
- http://www.nytimes.com/2009/04/30/science/30cyber.html?_r=1
- http://www.thetrumpet.com/?q=5940.4309.0.0
- http://blogs.govinfosecurity.com/posts.php?postID=236
- http://patdollard.com/2009/07/israelis-plot-cyber-war-on-iran/
- http://www.reuters.com/article/gc08/idUSTRE5663EC20090707?pageNumber=1&virtualBrandChannel=0&sp=true
- http://www.darknet.org.uk/2009/07/military-communications-hacking-script-kiddy-style/
- http://en.wikipedia.org/wiki/Stalking_horse
- http://en.wikipedia.org/wiki/Titan_Rain

- I LOL'ed http://neteffect.foreignpolicy.com/posts/2009/04/11/writing_the_scariest_article_about_cyberwarfare_in_10_easy_steps