

# Cyber Terrorism Fact or Fiction?

Mehdi M. Hassanzadeh

University of Bergen

Selmer Center

Norway

NISNet-Winter School in Information Security, Finse, May 22-27, 2011  
Selmer Center (University of Bergen), 18-19 Nov. 2010, Bergen, Norway

# Introduction

- With over **1.97 billion persons on the Internet** (Internet World Stats, 2011)
- Moreover, given the way the **Internet has affected everything** from booking a hotel to finding a partner, it is not surprising to see changes in the practice of terrorism.
- Indeed, the Internet is fundamentally transforming terrorism:
  - The way terrorists **disseminate** documents and propaganda
  - **Recruit** and **train** new members
  - **Inflict harm** on their victims

# Cyber **Terrorism**-Fact or Fiction?

- Activism
- Hacktivism
- Cyber War
- Cyber Terrorism



# Activism



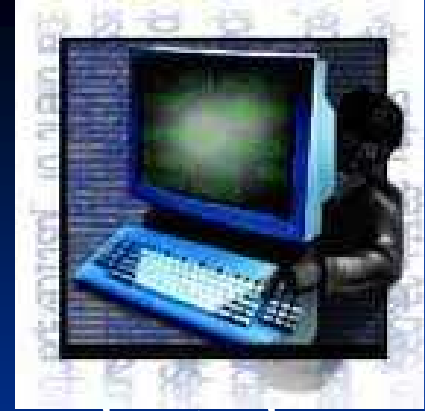
- Activism refers to normal, non-disruptive use of the Internet in support of an agenda or cause.
- Operations in this area include:
  - Browsing the Web for information
  - Constructing Web sites and posting materials on them
  - Transmitting electronic publications and letters through e-mail
  - Using the Net to discuss issues, form coalitions, and plan and coordinate activities.

# Hacktivism

- Hacktivism = Hacking + Activism
- It covers operations that use hacking techniques against a target's internet site with the intent of **disrupting** normal operations **but not causing serious damage**
  - Web sit-ins and virtual blockades
  - Automated e-mail bombs
  - Web hacks
  - Computer break-ins
  - Computer viruses and worms



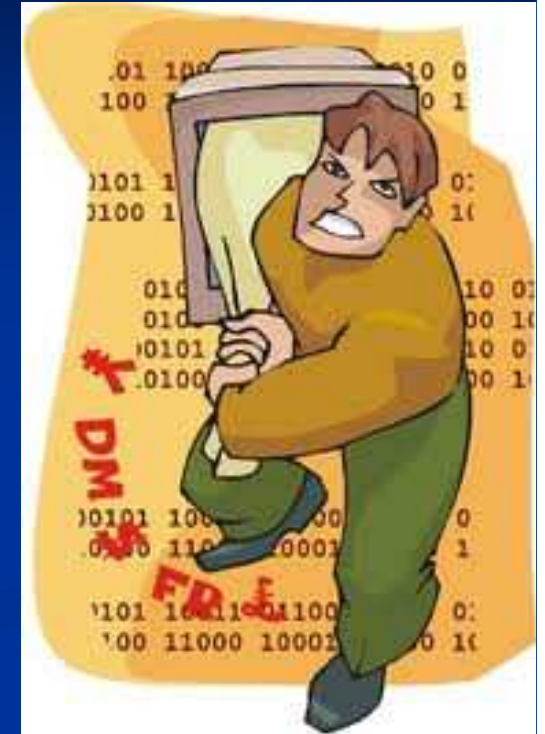
# Hacktivism: Virtual Sit-Ins and Blockades



- On December 21, **1995**, Strano Network group conducted one of the first such demonstrations as a protest against **French government** policies on nuclear and social issues.
- In **1998**, the Electronic Disturbance Theater organized a series of Web sit-ins, first against **Mexican President Zedillo**'s Web site and later against **President Clinton**'s White House Web site, the *Pentagon*, the School of the *Americas*, the *Frankfurt* and *Mexican Stock Exchange*.
  - The purpose was to demonstrate solidarity with the Mexican Zapatista
- In **1999**, the **Kosovo** conflict, both side use this technique

# Hacktivism: E-Mail Bombs

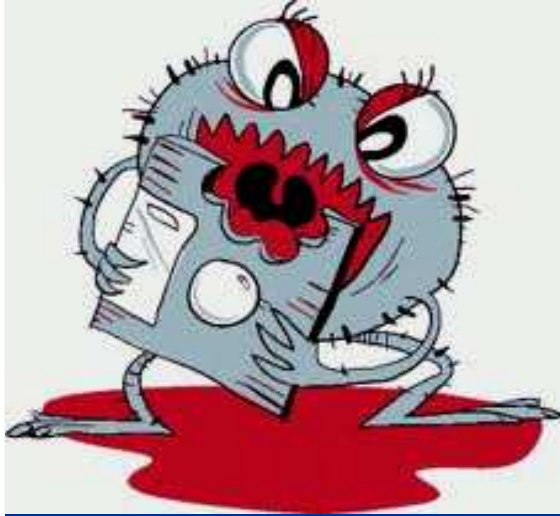
- The e-mail bombing consisted of about **800 e-mails** a day for about two weeks.
- During the **Kosovo conflict**, protestors on both sides e-mail bombed government sites, 1999.
  - NATO's server had been saturated at the end of March by **2,000** messages per day by **Belgrade** hackers.
  - California resident Richard Clark retaliated by sending **500,000** e-mails during a few days to the **Yugoslav government's** site and the site went down.



# Hacktivism: Web Hacks

- The media is filled with stories of hackers gaining access to Web sites and replacing some of the content with their own.
- See the [statistic](#) from Zone-h.org





# Hacktivism

## Viruses and Worms



- You can download free software programs from the Internet that create a virus for you.
- The first protest to use a worm occurred on October 16, **1989**, when anti-nuclear hackers released a worm into the U.S. National Aeronautics and Space Administration SPAN network.
- The **Code Red** worm, which infected about a million servers in July and August, **2001**, and caused \$2.6 billion in damages, was a single incident.
- **Stuxnet**: It was designed and released by a government--the Israel (unit 8200)--specifically to attack the Bushehr nuclear power plant in Iran. (**2010**)
  - looks for a particular model of PLC made by Siemens
- **Stars**: Its target is executive files of governmental organizations (**2011**)

# What is the Cyber War?

- Cyberwar is a form of war which takes places on computers and the Internet, through electronic means rather than physical ones.
- Some times it is supported by governments
- Weapons:
  - Keyboard
  - Mouse
  - Internet
- Operation:
  - Hacktivism



# The First Cyber War

- In 1997 when an offshoot of the Liberation Tigers of Tamil Eelam (LTTE) claimed responsibility for “suicide email bombings” against Sri Lankan embassies over a two-week period.
- Calling themselves the Internet Black Tigers, the group swamped Sri Lankan embassies with about 800 emails a day.
- The messages:

*“We are the Internet Black Tigers and we’re doing this to disrupt your communications.”*



# Cyberwar in Kosovo

- The conflict over **Kosovo** in 1999 has been characterized as the first war on the Internet.
- Government and non-government actors alike used the Net:
  - To disseminate information
  - To spread propaganda
  - To demonize opponents
  - To solicit support for their positions



# Cyberwar in Kosovo (cont.)

- Hackers used the Net to voice their objections to both **Yugoslav** and **NATO** aggression by disrupting service on government computers and taking over their Web sites.
- Most of the cyber attacks took the form of **web defacements** and **DoS attacks**.
- **Serb Black Hand** group crashed a **Kosovo** Albanian web site, justifying their actions with the statement “*We shall continue to remove ethnic Albanian lies from the Internet*”
- They also planned daily actions against NATO computers and **deleted data on a Navy computer**

# Pakistani-Indian Cyberwar

- It first started in May 1998, when India conducted its nuclear tests.
- A group of hackers called **milw0rm** broke into the Bhabha Atomic Research Center web site and posted anti-India and anti-nuclear messages.
- Then, **IGCOE** Hacker from India hacked Punjabi Pakistani Police official website.
- This cyberwar is never going to stop. This has infected several countries across the globe.

# Israeli-Palestinian Cyberwar

- The **Israeli-Palestinian** conflict has provoked numerous cyber attacks from hackers on both sides of the conflict.
- This was especially intense during the Second Intifada, which erupted in late **September 2000**.
- Most of the cyber attacks took the form of **web defacements** and **DoS attacks**.
- According to iDefense, over **40 hackers** from **23 countries** participated in this cyberwar during the period **Oct. 2000**, to **Jan. 2001**.

# U.S.-alQaeda Cyberwar

- Shortly after the **Sep. 11, 2001**, terrorist attack against the United States, hackers took to the Internet to voice their rage.
- A group called the Dispatchers announced they would destroy Web servers and Internet access in Afghanistan and target nations that support terrorists.
- Led by a 21-year-old security worker "Hackah Jak" from Ohio, the group of 60 people worldwide defaced **hundreds** of Web sites and launched denial of service attacks against such targets.

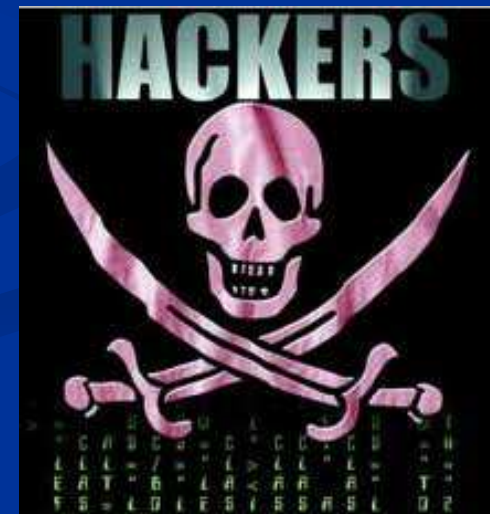


# U.S.-alQaeda Cyberwar

- Another group, called Young Intelligent Hackers Against Terror (YIHAT), claimed they penetrated the systems of **two banks** with ties to Osama bin Laden, although officials from the banks denied any security breaches occurred.
- **GForce Pakistan** announced the formation of the Al-Qaeda Alliance Online on a U.S. government website it had just defaced.
- Al-Qaeda has online training for new members to learn hacking and cyberwar

# Cyber War: Denmark

- In February 2006, Zone-h has recorded over **two thousand** web defacements, many in Denmark
- It was started to protest the twelve cartoons satirizing the Prophet Mohammad that were first published in the Danish newspaper *Jyllands-Posten*.



# Other examples of Cyberwar



- **Chinese-Taiwanese** Cyberwar (1999)
- **Chinese-American** Cyberwar (2001)
- **Russian-Estonian** Cyberwar (2007)
- **Russian-Georgian** Cyberwar (2008)
- Protest against the results of the **Iranian** political election (Twitter) (2009)
- **Japanese-S. Korean** Cyberwar (2010)
- **Indian-Bangladeshi** Cyberwar (2010)

# Other examples of Cyberwar



- Chinese-Japanese Cyberwar
- Chinese-Indian Cyberwar
- Turkish-Israeli and Armenian Cyberwar
- Turkish-Armenian Cyberwar
- Pakistani-Israeli Cyberwar
- Indian-Pakistani Cyberwar over the conflicts in the Middle East and Kashmir
- Google-Baidu Cyberwar (search engine)



# Ranking in Cyberwar

- The **majority** of the **attacks** came from persons in the **United States**, followed by **South Korea**, **China**, **Germany** and **France** (2002)
- As for the sources of **attacks per person**, **Israel** was the largest source, followed by **Hong Kong**, **Thailand**, **South Korea**, **France** and **Turkey** (2002)

# The Most Dangerous Countries Online

- AVG Technologies (2010):
  1. Turkey (1 in 10 users)
  2. Russia (1 in 14 users)
  3. Armenia (1 in 24 users)
  4. Azerbaijan (1 in 39 users)
  5. Bangladesh (1 in 41 users)
  6. Vietnam and Laos (1 in 42 users)

# What about other major Western countries?

- **AVG Technologies (2010):**
  1. **United States:** Global rank 9, (1 in 48 users)
  2. **UK:** Global rank 31, (1 in 63 users)
  3. **Australia:** Global rank 37, (1 in 75 users)
  4. **Germany:** Global rank 41, (1 in 83 users)

# The safest Countries Online

- AVG Technologies (2010):
  1. Sierra Leone (1 in 692 users)
  2. Niger (1 in 442 users)
  3. Japan (1 in 404 users)
  4. Taiwan (1 in 248 users)
  5. Argentina (1 in 241 users)
  6. France (1 in 224 users)
  7. Israel (1 in 210 users)

# Analyzing the data by continent

- AVG Technologies (2010):
  1. North America (1 in 51 users)
  2. Europe (1 in 72 users)
  3. Asia+Asia Pacific (1 in 102 users)
  4. Africa (1 in 108 users)
  5. South America (1 in 164 users)

# Under Attack!



WITH THE RISK OF WEB ATTACKS POSING A REAL THREAT AROUND THE GLOBE, WE DISCOVER THE RISKIEST AND SAFEST CONTINENTS TO GO SURFING



## CHANCES OF BEING ATTACKED

### BY CONTINENT

North America	1 in 51
Europe	1 in 72
Asia Inc. Asia Pacific	1 in 102
Africa	1 in 108
South America	1 in 164

### SAFEST COUNTRIES

1.	Sierra Leone	1 in 696
2.	Niger	1 in 442
3.	Japan	1 in 403
4.	Togo	1 in 359
5.	Namibia	1 in 353

### RISKIEST COUNTRIES

1.	Turkey	1 in 10
2.	Russia	1 in 15
3.	Armenia	1 in 24
4.	Azerbaijan	1 in 39
5.	Bangladesh	1 in 41

### SELECTED OTHERS

9.	America	1 in 48
30.	UK	1 in 63
36.	Australia	1 in 75
79.	China	1 in 135
98.	Brazil	1 in 155
118.	Czech	1 in 183





- McAfee: Cold cyber war involving the **United States, China, Russia, France** and **Israel** is already under way

# Why are there so many attacks?



- As the Internet has grown, there are **more people** out there to attack and **more sites** that are potential victims.
- The number of **vulnerabilities** in the systems. Microsoft, Linux and others all have vulnerabilities.
- User practices create vulnerabilities. **Bad passwords** are still a major plague on the Internet. A surprising number of people haven't even changed the default passwords.

# Cyberterrorism



# What is the mean by Cyberterrorism?



- In the 1980s, for the first time, **Cyberterrorism** was referred to the convergence of **cyberspace** and **terrorism** by Barry Collin, a former intelligence officer in U.S.
- It covers politically motivated hacking operations intended to cause grave harm such as **loss of life** or **severe economic damage**.
- The attack should be sufficiently **destructive** or **disruptive** to generate fear **comparable** to that from physical acts of terrorism.
- Extended power outages, plane crashes, water contamination, or major economic losses

# Several Possible Scenarios for Cyberterrorism



- In a 1997 paper, Barry Collin describes several possible scenarios for cyberterrorism
  - In one, a cyberterrorist hacks into the processing control system of a **cereal manufacturer** and changes the levels of iron supplement. A nation of children get sick and die.
  - In another, a cyberterrorist attacks the next generation of **air traffic control systems**. Two large civilian aircraft collide.
  - In a third, a cyberterrorist **disrupts banks, international financial transactions, and stock exchanges**.

# Examples of cyberterrorism



- The **Frankfurt** and **Mexican** Stock Exchange, 1998
- Attack on the **Russian** Stock Exchange, 2000
- In February of 2000, Amazon, Yahoo, eBay, ETrade, ZDNet, CNN.com, Buy.com, and Excite were hit by massive DOS assaults aided by trinoo, TFN, and Stacheldraht.
- The e-commerce suffered losses of **\$1.2 billion.**
  - \$1 billion represented market capitalization losses
  - \$100 million lost revenue from sales and advertising
  - \$100 to \$200 million security upgrades

# Examples of cyberterrorism (Cont.1)

- In Australia (2000), A man penetrated the Maroochy Shire Council's **waste management system** and used radio transmissions to alter pump station operations.
- A **million liters of raw sewage** spilled into public parks and creeks on Queensland's Sunshine Coast
- **Killed marine life**, turned the water black, and created an unbearable stench



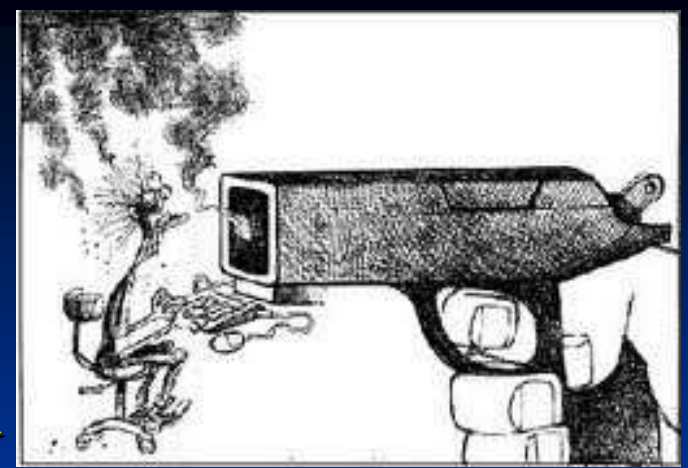
# Examples of cyberterrorism (Cont.2)

## ■ Against **Iran**

- **Stuxnet** Worm 2010: Stuxnet malware (spyware) is 'weapon' out to destroy ... Iran's Bushehr nuclear plant!
  - Iran Deny Nuclear Station Hit
- Attack to the power supply in Iran
  - We had outage in Tehran and several big city for several hours
  - There is no news about the reason: Cyber attack or technical failure?



# Is the Cyberterrorism the way of the future?



- It could be conducted **remotely** and **anonymously**
- It would be **cheap**
- It would not require the handling of **explosives** or a **suicide mission**
- There are no **instances** of cyberterrorism
- It is **not possible** to assess the impact of acts that have taken place



# How we can assess the potential threat of cyberterrorism

- Whether there are targets that are **vulnerable** to attack that could lead to severe harm. Eight infrastructures were identified:
  - Telecommunications, banking and finance, electrical power, oil and gas distribution and storage, water supply, transportation, emergency services, and government services.
- Whether there are **actors** with the capability and motivation to carry them out.
  - Religious, New Age, Ethno-nationalist separatist, Revolutionary, Far-right extremist, and Cyber protests



# Cyber Command

- **Mission:** coordinate, integrate, synchronize and conduct activities against the Cyberterrorim.
  - **US:** CYBERCOM (2009)
  - **Iran** (2011)
  - **Israel:** Unit 8200 is an Israeli Intelligence Corps unit (**Stuxnet**), established CC in 2011.
  - Some **European countries** have also established similar organizations to counter cyber threats posed to their interests

# Conclusion



- Cyber terrorism is certainly a real possibility, for a terrorist, digital attacks have **several drawbacks**. Systems are complex, so controlling an attack and achieving a desired level of damage may be harder than using physical weapons.
- The evidence shows that terrorist groups have an **interest** in conducting cyber attacks.
- Further, they are **attempting to develop** and deploy this capability through online training.
- Terrorists have not yet demonstrated that they have the **knowledge and skills** to conduct highly damaging attacks against critical infrastructures, but **government** can do it.
- **The evidence shows that cyberterrorist is started in the world now.**

**Thank you for your attention**

Question?



# Reference



1. Dorothy E. Denning, “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy”, June 8, 2001, <http://www.cs.georgetown.edu/~denning>
2. Schneier on Security: <http://www.schneier.com/blog/archives/2010/10/stuxnet.html>
3. Dorothy E. Denning, “The Web Ushers In New Weapons of War and Terrorism”, August 18, 2008.
4. Dorothy E. Denning, “Is Cyber Terror Next?”, November 1, 2001, <http://essays.ssrc.org/sept11/essays/denning.htm>
5. The Computer Emergency Response Team Coordination Center (CERT/CC): <http://www.cert.org/cert/>
6. <http://www.Zone-h.org>
7. Dorothy E. Denning , “Terror’s Web: How the Internet Is Transforming Terrorism”, 2009.
8. “Sewage Hacker Jailed,” *Herald Sun*, October 31, 2001.