Cyber Terrorism: Fact or Fiction?

Financial Services
Information Sharing and Analysis Center

Presentation to the
New England Disaster Recovery Information X-Change

June 13, 2005

Byron Collie
Vice President, Goldman Sachs
Chair, FS/ISAC Threat & Intelligence Committee

Dan DeWaal
Vice President, Options Clearing Corporation
Member, FS/ISAC Threat & Intelligence Committee
Disclaimer

Material contained in this brief is provided by the FS/ISAC Threat & Intelligence Committee for discussion purposes only.

The comments and the opinions expressed in this presentation are those of the authors and may not reflect those of Goldman Sachs or Options Clearing Corporation.
Overview

• FS/ISAC
• Define “Cyber terrorism”
• How terrorists use computers
  – Indirect Support
  – Operational Support
  – Computers as the Target
• Capability
• Access is the Key!
• Cyberwars and E-Jihads
• Palestinian/Israeli Cyberwar
• Cyber Terrorism vs Physical Terrorism
• The Reality
• Summary
What is the FS/ISAC?

- Financial Services Sector Information Sharing and Analysis Center - FS/ISAC.

- Organization designed and developed by industry professionals after Presidential Decision Directive 63 was issued in 1998. PDD 63 was designed to create a public and private sector partnership to protect the critical infrastructure of the United States.

- FS/ISAC became operational in October 1999 and was restructured in 2003 to broaden its mission and serve all financial services sector participants.

- The FS/ISAC is a 501(c)6 nonprofit corporation owned and operated by the private sector to help protect the critical infrastructure of the United States.
What is the FS/ISAC’s Mission?

Mission Statement

To disseminate trusted and timely information intended to increase sector wide knowledge about physical and cyber security operational risks faced by the Financial Services Sector.
Definition of Terrorism

Section 212(a)(3)(B) of the Immigration and Nationality Act (INA) defines ‘terrorist activity’ as:

"any activity which is unlawful under the laws of the place where it is committed (or which, if committed in the United States, would be unlawful under the laws of the United States or any State) and which involves any of the following:

(I) The highjacking or sabotage of any conveyance (including an aircraft, vessel, or vehicle).

(II) The seizing or detaining, and threatening to kill, injure, or continue to detain, another individual in order to compel a third person (including a governmental organization) to do or abstain from doing any act as an explicit or implicit condition for the release of the individual seized or detained.

(III) A violent attack upon an internationally protected person (as defined in section 1116(b)(4) of title 18, United States Code) or upon the liberty of such a person.

(IV) An assassination.

(V) The use of any--

   (a) biological agent, chemical agent, or nuclear weapon or device, or

   (b) explosive, firearm, or other weapon or dangerous device (other than for mere personal monetary gain), with intent to endanger, directly or indirectly, the safety of one or more individuals or to cause substantial damage to property.

(VI) A threat, attempt, or conspiracy to do any of the foregoing."
Defining “Cyber terrorism”

- There is no standard US Government definition of “Cyber terrorism”

- National Infrastructure Protection Center (NIPC), now within DHS, defined cyber terrorism as:
  
  “a criminal act perpetrated through computers resulting in violence, death and/or destruction, and creating terror for the purpose of coercing a government to change its policies.”

- Dorothy E. Denning Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives:
  
  “. . . unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives.”

- The working definition presented to Congress in 2003 is:
  
  “The politically motivated use of computers as weapons or as targets, by sub-national groups or clandestine agents intent on violence, to influence an audience or cause a government to change its policies..”
## Who are the terrorists? (Dept of State)

- Abu Nidal Organization (ANO)
- Abu Sayyaf Group
- Al-Aqsa Martyrs Brigade
- Armed Islamic Group (GIA)
- Asbat al-Ansar
- Aum Shinrikyo
- Basque Fatherland and Liberty (ETA)
- Gama’a al-Islamiyya (Islamic Group)
- HAMAS (Islamic Resistance Movement)
- Harakat ul-Mujahidin (HUM)
- Hizballah (Party of God)
- Islamic Movement of Uzbekistan (IMU)
- Jaish-e-Mohammed (JEM) (Army of Mohammed)
- al-Jihad (Egyptian Islamic Jihad)
- Kahane Chai (Kach)
- Kurdistan Workers’ Party (PKK) a.k.a. Kurdistan Freedom and Democracy Congress (KADEK)
- Lashkar-e Tayyiba (LT) (Army of the Righteous)
- Lashkar i Jhangvi
- Liberation Tigers of Tamil Eelam (LTTE)
- Mujahedin-e Khalq Organization (MEK)
- National Liberation Army (ELN)
- Palestinian Islamic Jihad (PIJ)
- Palestine Liberation Front (PLF)
- Popular Front for the Liberation of Palestine (PFLP)
- PFLP-General Command (PFLP-GC)
- al-Qa’ida
- Real IRA
- Revolutionary Armed Forces of Colombia (FARC)
- Revolutionary Nuclei (formerly ELA)
- Revolutionary Organization 17 November
- Revolutionary People’s Liberation Army/Front (DHKP/C)
- Salafist Group for Call and Combat (GSPC)
- Shining Path (Sendero Luminoso, SL)
- United Self-Defense Forces of Colombia (AUC)
- Communist Party of the Philippines/New People’s Army (CPP/NPA)
- Jemaah Islamiya organization (JI)
How can terrorists use computers?

Three majors ways terrorists can make use of computer systems:

1. Indirect Support of overall group.

2. Operational Support of terrorist activities.

3. Specifically as a target for destruction or disruption.
Indirect Support

- **Propaganda**
  - Spread their message
  - Advocate jihad and terror

- **Fund-raising**
  - Appeal for donations – money, weapons
  - Sometimes disguised as charitable contributions through a charity front
  - Some using electronic crime techniques such as *phishing* to provide financial support.

- **Recruiting**

- **Example sites**
  - almuhajiroun.com
  - azzam.com
al-Qaida and Osama bin Laden -- funded the bombing of the World Trade Center in New York in 1993, the Khobar Towers in Saudi Arabia in 1996, and the American embassies in Kenya and Tanzania in August, 1998. The release of a videotape in late 2001 left little doubt that bin Laden was behind the attacks of September, 2001. "The organization that eventually evolved into al-Qaida (the name means 'the base' in Arabic) began as the Makhub al Khadinat, the Office of Services, the Peshawar, Pakistan [...]" ["New York Times", 9 June 2002, pp 1,26,27].

- **Al-Muhajiroun** supports bin Laden: [http://www.almuhajiroun.com](http://www.almuhajiroun.com)
- Plenty of Osama bin Laden support, plus zip files with 1000-page Jihad how-to manuals: [http://bootdown.trouble-free.net/~jehad/](http://bootdown.trouble-free.net/~jehad/)
- Many groups labeling themselves as part of the Khilafah movement support bin Laden and the Taleban:
  - [http://turn.to/khilafah](http://turn.to/khilafah)
  - Two collections of pages with some identical content:
    - [http://www.raisedeen.8k.com](http://www.raisedeen.8k.com)
- **Almeda.com** is all in Arabic, but it is said (e.g., by *Jane's international analysis*) to have been publishing "a
Operational Support

- For intelligence collection to support physical or cyber attacks:
  - al-Qaeda used Web to research targets and techniques
    - Pilot training
    - Crop-dusting
    - Financial services buildings in NY and NJ
- For communication:
  - Zacarias Moussaoui’s laptop contained a list of all the hijackers involved in the September 11 attacks
  - His email address was xdesertman@hotmail.com
Operational Support

- The Provisional Irish Republican army used the Internet as a tool to organize plans to plant bombs in six electrical subway stations last year around London, according to Vatis. If the terrorists were successful, they would have crippled the transportation system of much of London and South West England.

  - Michael Vatis, Deputy Assistant Director & Chief, Federal Bureau of Investigation (FBI)
  16 April 1998
Computers As Targets

- Most likely targets, critical infrastructure related computer systems and networks.
- Attacks against systems and networks will normally be transitory events due to backups, BCP etc.... unless...... the system or network being attacked can have some measurable impact in the physical world:
  - Supervisory Control and Data Acquisition (SCADA) systems for utilities such electricity, water etc
  - Traffic light control systems
  - Air Traffic control systems
  - Activities where communications are crucial in preventing physical events (again air traffic control is a good example)
  - Where denied communications can have substantial business/financial impact (Stock Exchange trading for example)
Naval Postgraduate School: Cyber terrorism Study

- Center for the Study of Terrorism and Irregular Warfare, Naval Postgraduate School (CSTIW/NPS)
  - Assessed prospects of terrorist organizations pursuing cyber terrorism
  - Conclusions:
    - Barrier for entry for anything beyond annoying hacks is high
    - Terrorists generally lack the wherewithal & human capital
    - Cyber terrorism is thing of future, but might be pursued as ancillary tool

Credit for extract to Dorothy E. Denning, Georgetown University
Why use Cyber terrorism?

• Tighter physical security measures now widely in place may actually encourage terrorists in the future to explore cyber terror as a form of attack that offers lower risk of detection to the attackers, with effects that could possibly cascade to disrupt other information systems throughout the critical infrastructure.

• To be successful, the cyber terrorist would need two to have:
  – Intent, and
  – Capability

• Terrorists are not lacking in the first but they are lacking in the second.
Levels of Capability (from NPS Study)

- **Simple-unstructured**
  - Conduct basic hacks using available tools

- **Advanced-structured (2-4 years to develop)**
  - Conduct more sophisticated attacks against multiple systems/networks; create or modify tools; target analysis, command and control, learning

- **Complex-coordinated (6-10 years to develop)**
  - Coordinated attacks causing mass disruption against integrated, heterogeneous systems; create sophisticated tools; advanced target analysis, command and control, learning

Credit for extract to Dorothy E. Denning, Georgetown University
Capability

- al-Qaida:
  - 22 Jan 2004 CNN “Man linked to al-Qaida indicted”:
    - "A Minnesota man has been indicted on charges he provided material support to al Qaeda for more than three years, the Justice Department said Wednesday."
    - Authorities say Mohammed Abdullah Warsame, 30, attended an al Qaeda training camp in Afghanistan at which Osama bin Laden was present.
    - Warsame had worked as a computer science tutor at Minneapolis Community Technical College, Jamal said.

- Institute for Defense Analyses (IDA) believes:
  - 4th generation al-Qaida operatives are currently being fielded who are intelligent, educated, motivated and take the long view with respect to their activities.

- Question: How good is your background check program?
Capability

- Cyber weapons still relatively immature:
  - Malicious code (virii, worms, trojans)
  - Denial of Service attacks (short-lived these days)
  - Unauthorized Access – larger financial firms have good security. It is the smaller firms that have connectivity to the national financial infrastructure that likely pose the threat.

- Most firms have very hardened perimeters so remote access into environment would be problematic.
Access is the Key!

• With access, little technology required.
• Without access, no amount of technology will help.
• Most firms have very hardened perimeters so remote access into environment would be problematic.
• Insider most likely threat vector.
• Preventing access is key to defense.
  – Physical, personnel, and information.
• Physical and information security need to work hand in glove to correlate threats.
• This is a major theme for the FS/ISAC and Physical/Cyber Security Integration Seminars held in New York, Chicago and San Francisco.
Cyber Wars and E-Jihads

- Palestinian/Israeli
- Pakistan/India
- China/Taiwan
- Yugoslavia/Kosovo
- Muslim/US
- Primarily:
  - Denial of Services attacks against web sites
  - Web site defacements
- No evidence of sophisticated cyber weapons being developed
- Sites with good security, backups and business continuity plans little affected
Palestinian/Israeli Cyberwar

- From start in October 2000 - January 2001 [iDefense]
- Attackers from 23 countries hit 8 governments
- 16+ tools used – posted on supporting websites
- 30+ Pro-Palestinian attackers hit 166+ sites
  - commercial sector hit hardest (51%)
  - Unity, Muslim extremists with ties to Hezbollah
  - al-Muhajiroun, Muslim extremists with ties to bin Laden
  - 4-phases: 1) Israeli government sites, 2) Tel Aviv stock exchange and Bank of Israel, 3) Israeli ISP infrastructure, 4) Zionist e-commerce sites
- 10+ Pro-Israeli attackers hit 34+ sites
  - terrorists/extremists (Hamas, Hezbollah) hit hardest (39%)

Credit for extract to Dorothy E. Denning, Georgetown University
Internet Black Tigers offshoot swamped Sri Lankan embassies with 800 e-mail messages/day for 2 weeks

Characterized as first known attack by terrorists against a country’s computer systems

Credit for image to Dorothy E. Denning, Georgetown University
Cyber Terrorism vs Physical Terrorism

- **Cyber terrorism**
  - Remotely executable from the comfort of your own cave
  - Complex to plan and execute effectively
  - Few lasting effects
  - Attribution difficult due to jurisdictional issues globally
  - Impersonal, normally no physical impact directly on person
  - “Terror” difficult to induce in target audience as normally no threat to physical safety

- **Physical Terrorism**
  - Typically must get up close and personal
  - Most acts employ simple mechanisms (car bombs, suicide bombs, aircraft hijacking)
  - Planning may be simple depending on intended effect
  - Lasting effect (9/11 perfect example)
  - “Terror” easily induced in target audience due to fear for safety
Someday soon, several bands of small terrorist cells will gather together in a cave to blow up the Internet...
What is the reality?

  
  "Currently no evidence exists that terrorist organizations are actively planning to use computers as a means of attack, and there is disagreement among some observers about whether critical infrastructure computers offer an effective target for furthering terrorists’ goals."

  "Some security experts believe that past discussions about cyber terrorism may have over-inflated the perceived risk to the critical infrastructure."

- Cyber attacks currently have a poor fit to normal terrorist objectives.

- DHS considers that cyber terrorist capabilities will continue to develop in the near future.
Summary

• Cyber terrorism is an overused term that has no standard definition.

• Fact: There has not been one quantifiable act of cyber threat activity where terror has been induced in a target audience.

• Fact: Compared to physical acts of terrorism, cyber terrorism is more complex to plan and execute.

• Fact: A cyber security action by a terrorist is likely to be carried out in support of some physically directed activity rather than as a standalone activity.

• **Reality:** Companies should treat cyber terrorism as a realistic future threat but not panic. How rapidly the threat will develop though cannot be predicted, so...

• Companies should **NOW** evaluate their security posture and develop integrated policies and procedures that support business continuity plans.

• Build trust relationships with public and private organizations by participating in organizations like NEDRIX and FS/ISAC.
References

- “Terrorists & the Internet” Dorothy E. Denning, Georgetown University http://www.cs.georgetown.edu/~denning/infosec/Denning-Cyberterror-SRI.ppt
QUESTIONS?

byron.collie@gs.com
ddewaal@theocc.com