



# *Cyber Terrorism: Myth or Menace?*

**Irving Lachow**

**May 15, 2008**



*“A global learning community for government’s most promising information leaders.”*



- **What is Cyber Terrorism?**
  - **Definition**
  - **Cyber Terror vs. Other Cyber Threats**
- **Is Cyber Terrorism a Serious Problem?**
- **How Are Terrorist Using the Internet?**
- **Is Terrorist Use of the Internet a Serious Problem?**
- **What are US Response Options?**
- **Discussion**

# What is Cyber Terrorism?

## ➤ Definitions of terrorism:

- State Dept: “Premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience.”
- FBI: “The unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”

## ➤ Definition of cyber terrorism:

- Denning: “A computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. *The attack should be sufficiently destructive or disruptive to generate fear comparable to that from physical acts of terrorism.* Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples... *Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.*”

# Cyber Terrorism vs. Other Cyber Threats

	<i>MOTIVATION</i>	<i>TARGET</i>	<i>METHOD</i>
Cyber Terror	Political or social change	Innocent victims	Computer-based violence or destruction
Hacktivism	Political or social change	Decision-makers or innocent victims	Protest via web page defacements or DDOS
Black Hat Hacking	Ego, personal enmity	Individuals, companies, governments	Often use malware, viruses and worms, and hacking scripts
Cyber Crime	Economic gain	Individuals, companies	Often use malware for fraud, ID theft; DDOS for blackmail, etc.
Cyber Espionage	Economic and political gain	Individuals, companies, governments	Use wide range of techniques to obtain information.
Info War	Political or military gain	Infrastructures, IT systems and data (private or public)	Use wide range of techniques for attack or influence operations.

- **What is Cyber Terrorism?**
- ***Is Cyber Terrorism a Serious Problem?***
  - ***Terrorism Risk Model***
  - ***Assessment of Current Risk***
  - ***Assessment of Future Risk***
- **How Are Terrorist Using the Internet?**
- **Is Terrorist Use of the Internet a Serious Problem?**
- **What are US Response Options?**
- **Discussion**

- **Risk = Threat\*Vulnerability\*Consequence**
  - **Threat = Probability that a given attack is launched against a given target**
  - **Vulnerability = Probability that a given attack against a given target succeeds**
  - **Consequence = Expected level of damage from a successful attack against a given target**
- **Countermeasures can be applied against any or all of these three variables**
  - **Countermeasures usually described in terms of three categories: Protect, Detect, Respond**
  - **A given countermeasures always carries costs/risks**

# Risk from Cyber Terrorism Is Currently Low

- **No documented cases of cyber terrorism in US or Europe**
- **Few indications that serious cyber terrorist threats are imminent**
- **Wargames by Gartner/NWC and NPS both showed that risks of cyber terror are overstated**
- **Most security experts agree**
  - Denning, Lewis, Libicki, Kohlman, Schneier, Weimann, Winkler...
- ***Why are risks lower than perceptions indicate?***

# Cyber Terrorism vs. Other Attack Vectors

## ➤ Cyber Terror Challenges:

- Nuisance attacks are easy but do not create desired effects
- Serious attacks are difficult to do and may create desired effects
  - Require extensive intelligence gathering, training, and funding
  - Require different skill sets and potential reliance on outside experts
  - Prospects for success and potential outcomes are highly uncertain
- Bottom line: costs outweigh benefits in most cases

## ➤ Explosives Work Very Well

- Easy to do, require little training, and ops are based upon extensive knowledge base
- Highly effective at creating terror and getting attention.

## ➤ WMD is Another Option

- Would create tremendous sense of terror and panic
- Would dominate news for weeks or months
- Would be huge source of pride

# Future Cyber Terrorism Risk May Be Greater

## ➤ Trends For Cyber Terror

- Demographics
- Growing risk of state sponsorship
- Outsourcing to hackers and criminals
- Increased reliance of infrastructures on Internet
- Growth in software vulnerabilities
- Technology trends

## ➤ Trends Against Cyber Terror

- Increasing focus on cyber security
- Growing resilience in infrastructures
- Technology trends
- Fundamental challenges remain in place

- **What is Cyber Terrorism?**
- **Is Cyber Terrorism a Serious Problem?**
- ***How Are Terrorist Using the Internet?***
  - ***Why the Internet?***
  - ***Organizational Effectiveness***
  - ***Influence Operations***
- **Is Terrorist Use of the Internet a Serious Problem?**
- **What are US Response Options?**
- **Discussion**

# Why Do Terrorists Use the Internet?

- **Rapid communications**
- **Low cost**
- **Ubiquity**
- **Ease of use + sophistication of tools**
- **Anonymity**
- **Social networking**

# How do Terrorists Use the Internet?

## ➤ Organizational effectiveness

- Communications
- Fundraising
- Training
- Command and control
- Intelligence gathering

## ➤ Influence Operations

- Create support in general population
- Recruiting
- Media relations
- Counter propaganda

**The Internet is enabling networked organizational structures that are extremely difficult to destroy.  
(Starfish vs. Spider)**

- **What is Cyber Terrorism?**
- **Is Cyber Terrorism a Serious Problem?**
- **How Are Terrorist Using the Internet?**
- ***Is Terrorist Use of the Internet a Serious Problem?***
- **What are US Response Options?**
- **Discussion**

# Consensus: U.S. is Losing Cyber War Against Terrorists

- **Terrorist use of Internet is leading to:**
  - A global ideological movement based on a set of guiding principles and beliefs
  - Effective operational structures that support local action without centralized control
  - Effective perception management campaigns that influence target audiences while undermining U.S. interests
- **Secretary of Defense Rumsfeld:**
  - “If I were rating, I would say we probably deserve a D or D+ as a country as how well we’re doing in the battle of ideas that’s taking place.”
- **Dr. Bruce Hoffman:**
  - “...the U.S. is dangerously behind the curve in countering terrorist use of the Internet...”

# Warfare in the Information Age Is a New Ball Game

- **US View = Clausewitz: “War is violence to constrain the enemy to accomplish our will”**
  - Information supports kinetics
  - Great for industrial age, not for information age
- **Terrorist View = Sun Tzu: “To win 100 victories in battles is not the acme of skill...To subdue the enemy without fighting is the acme of skill.”**
  - Kinetics support information
  - Great for information age, not for industrial age
- **Osama Bin Laden: “It is obvious that the media war in this century is one of the strongest methods; in fact, its ratio may reach 90% of the total preparation for the battles.” (Letter to Mullah Mohammed Omar, written prior to 2002)**
  - He gets it!

# Examples of Terrorist Use of the Internet

- **Growth in number and of sophistication of websites and videos**
  - **Number of web sites grew from around 12 to over 4300 in eight years (Weimann)**
  - **YouTube**
- **Evidence of Internet use for kinetic operations**
  - **9/11**
  - **London**
- **Evidence of kinetic operations supporting info war**
  - **See videos from Iraq**

- **What is Cyber Terrorism?**
- **Is Cyber Terrorism a Serious Problem?**
- **How Are Terrorist Using the Internet?**
- **Is Terrorist Use of the Internet a Serious Problem?**
- ***What are US Response Options?***
  - ***Cyber Terrorism***
  - ***Terrorist Use of the Internet***
- **Discussion**

# Treat Cyber Terror as “Lesser Included” Cyber Security Threat

- **Focus cyber defense efforts on hacking, crime, espionage, and state-level threats**
  - **These efforts will also work against cyber terrorism**
- **Improve resilience of critical infrastructures and key resources**
- **Use proven counter-terrorism techniques from intelligence and law enforcement**
- **Explore possible role of pre-emption and deterrence**

# Counter TUI Via Comprehensive Strategy

- **Develop high-level, coordinated strategy for countering terrorist use of the Internet**
  - **Current efforts are disjointed and occur mostly at operational and tactical levels**
- **Strategy must maximize benefits and minimize risks/costs of each layer of info environment (infrastructure, content, and cognition)**
  - **Where appropriate disrupt infrastructure to create fear, uncertainty, and doubt (FUD) about its reliability**
  - **Attack confidentiality, integrity and availability of extremist information to further increase FUD, gain intelligence and disrupt operations**
  - **Focus significant time, energy and resources on cognitive domain to impact terrorist decision-making, reduce terrorist influence on stakeholders, and promote US ideas**

# A Few More Recommendations

- **US alone cannot counter extremist Muslim ideology**
  - **Must build up and/or support networks of moderate Muslims and help spread their message**
  - **Use former terrorists to undermine extremist recruiting**
- **Need to reset terms of ideological struggle**
  - **Change language used to describe the players and their actions**
  - **Focus on things that matter to Muslim audiences (e.g., honor)**
- **US must adapt to fight a long-term, broad-based “war of ideas”**
  - **Elevate importance of information component of power in Executive**
  - **Develop structures, processes, incentives to better coordinate IO, PD, SC**
  - **Strengthen capabilities of diplomatic corps and the “non-kinetic” abilities of soldiers**

- **What is Cyber Terrorism?**
- **Is Cyber Terrorism a Serious Problem?**
- **How Are Terrorist Using the Internet?**
- **Is Terrorist Use of the Internet a Serious Problem?**
- **What are US Response Options?**
- **Discussion**

Dr. Irv Lachow  
Senior Research Professor  
Information Resources Management College  
National Defense University

Email: [lachowi@ndu.edu](mailto:lachowi@ndu.edu)

Office phone: (202) 685 - 2060

Cell phone: (202) 903 - 7722