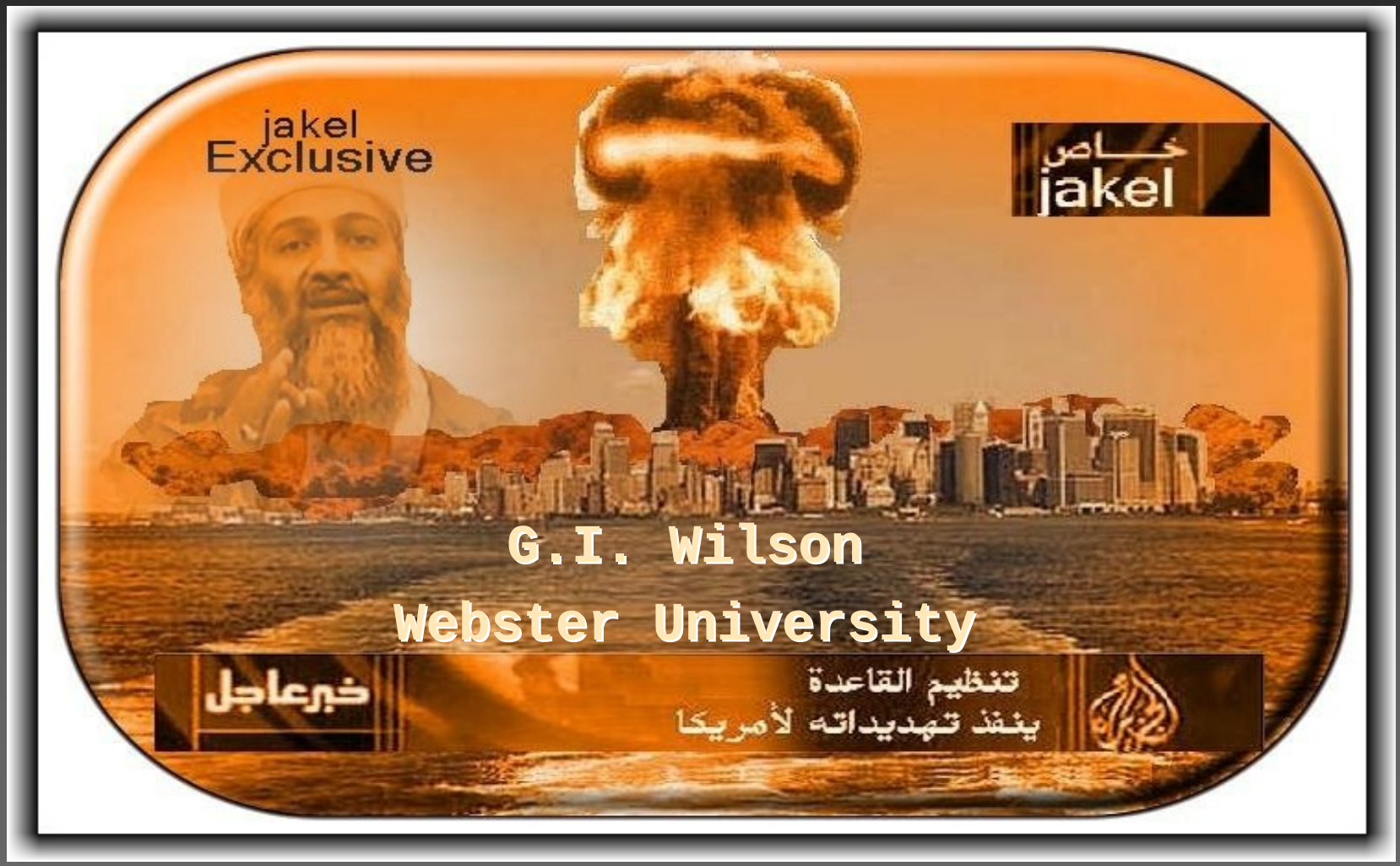
Terror's Digital Jihad



Introduction

- ✓ **Globalization** and the **Internet** are accelerating terrorist activity and their quest for digital jihad.
- ✓ Terrorists use the Internet to achieve many of their objectives.

Introduction

“ The Internet allows small groups of non-state foes to finance, plan, supply, and execute terrorist operations globally with little regard to borders, laws, and governments. ”

John Robb, *Brave New War*

What Is The Threat ?

To **determine the threat** this paper examines:

- Terrorists' use of the Internet
- Cyber terrorism

Definitions: Terrorism and Cyber Terrorism

- No universal accepted definition of terrorism.
- Marsella defines terrorism “as the **use of force or violence**, by individuals or groups that is directed toward civilian populations and intended to **instill fear** as a means of **coercing individuals or groups to change their political and social** positions”.

Definitions: Terrorism and Cyberterrorism

- Like terrorism, cyberterrorism has different connotations.
- Denning holds that cyberterrorism " refers to highly damaging **computer-based attacks** or threats of attack.

  By non-state actors against information systems when conducted **to intimidate or coerce** governments or societies in pursuit of goals that are **political or social**" .
- What distinguishes cyberterrorism from cyber war is that **non-state actors** undertake **cyberterrorism**, whereas **nation states** undertake **cyber war**.

Brief Literature Survey

The Center on Terrorism and Irregular Warfare Monterey, California conducted one of the first comprehensive surveys of cyber terrorism

The Center's original assessment and follow-on work found that terrorist have at best a marginal and cursory capability to carry out cyber terrorism.

Dr Denning in her 2007 assessment, *A View of Cyberterrorism Five Years Later*, reaches much the same conclusion as well as others.

Current literature and research **evidence simply does not support an imminent threat of cyber terrorism.**

Electronic Jihad

While suicide attacks and improvised explosives devises (IED) remain popular with terrorists, this does not mean we ignore the threat of cyber terrorism.

The Jamestown foundation reports how electronic jihad which is organized and coordinated attacks to wage economic and ideological warfare is be promoting on the internet.

Dr. Alshech contends that while electronic jihad is capable of causing some moderate damage to western economy, there is no indication of an immediate threat.

Internet Not A Terrorist Target

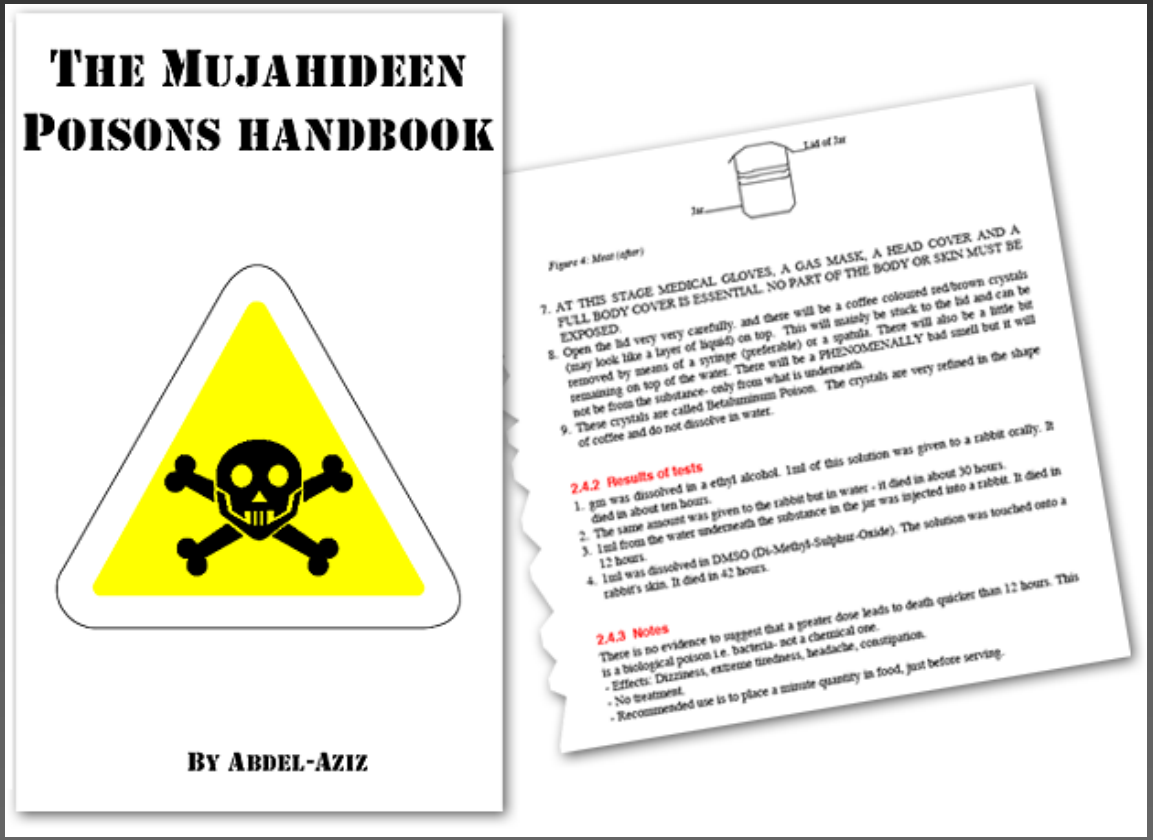
While the electronic jihad promotes coordinated cyber attacks using the Internet,but, the Internet itself is not a terrorist target.

For terrorist the Internet is a **computer-mediated communication (CMC)** platform for:

- Recruiting
- Training
- Funding
- Targeting
- Information operations
- Intelligence collection

Computer-Mediated Communication (CMC)

Online Poisons Handbook



Convergence: Terrorism,Crime, and Internet

- ✓ Terrorists have found that the Internet and criminal activity (e.g. drug trafficking, financial scams, cyber-crime, illegal money transfers, identity theft) gives them “discrete advantages”.
- ✓ For example, using the Internet and ATMs to move money illustrates the creativity and sophistication of terrorists and criminals.
- ✓ An example how terrorism,crime, and the Internet converge is found in the Bali disco bombing.

Bali Indonesia Disco Bombing

Terrorism + Crime + Internet = Operational Funding

Two hundred two people died in the Bali, Indonesia, disco bombing of October 12, 2002, when a suicide bomber blew himself up on a tourist-bar dance floor, and then, moments later, a second bomber detonated an explosives-filled Mitsubishi van parked outside. Now, the mastermind of the attacks—Imam Samudra, a 35-year-old Islamist militant with links to al--Qaeda—has written a jailhouse memoir that offers a primer on the more sophisticated crime of online credit card fraud, which it promotes as a way for Muslim radicals to fund their activities.

NetWar, Networking, and Information Security

- ✓ The Internet provides non-state actors a place and a means to expand their influence, social network, and operational reach.
- ✓ Arquilla and Ronfeldt defined “netwar” as unconventional decentralized warfare: nontraditional warfare carried out by dispersed groups of activists (i.e. terrorists, criminals, gangs, tribes, clans, militias) without a central command. They often communicate and coordinate electronically via the Internet.
- ✓ Sullivan posits that netwar may result in a distinct and perhaps "refined form of terrorism" where "inter-netted' transnational criminal organizations (TCOs), triads, cartels, cults, terrorists, gangs and other entities replace their more state-oriented predecessors.

Information and Operational Security (OPSEC)

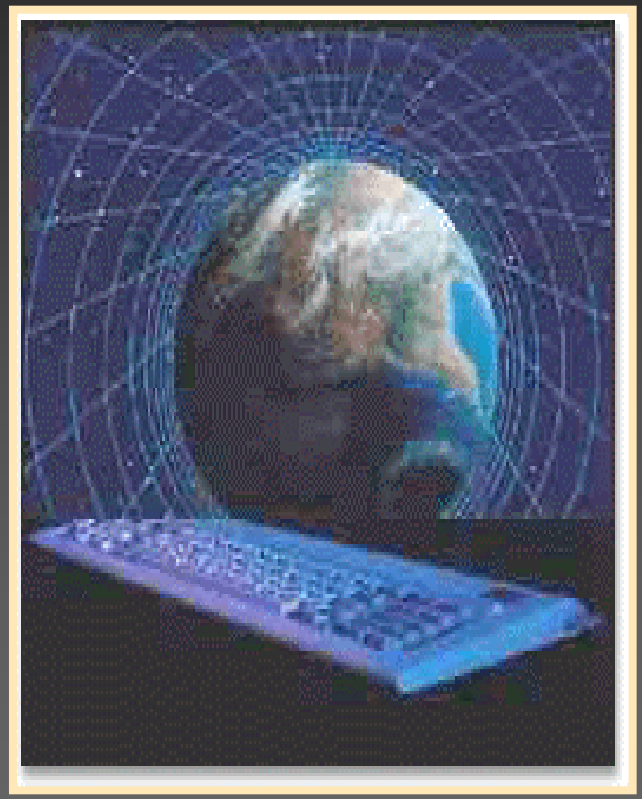
- ✓ A terrorist survival kit used by Al Qaeda and the Taliban contained instructions on information and operational security (OPSEC) for Internet and network communications. “Internet use follows protocols based on using public Internet cafés…never going to the same café repeatedly and not using messages that will betray your ideological commitment”

- ✓ Zanini and Edwards note that terrorist networks information security is bolstered by commercial encryption programs.

- ✓ Denning observes there are reports suggesting jihadists are using steganography and an issue of the *Technical Mujahid* refers to steganography.

Social Engineering

- Social engineering is a compilation of techniques used to influence and manipulate people into divulging or exposing guarded, sensitive, or confidential information.
- Social engineering is similar to a confidence or fraud scam and typically involves trickery, ruses, and deception for the purpose of gathering sensitive information or gaining access to computer network systems.



Social Engineering

Using social engineering techniques trio stole more than **37,000 credit card numbers**:

- $3.5 million in fraudulent charges and purchases.
- Hundreds of prepaid cell phones acquired.
- More than 250 airline tickets using 110 different credit cards at 46 airlines and travel agencies obtained.

Left to right, Waseem Mughal, Younis Tsouli and Tariq al-Daour. The three men pleaded guilty to a terrorism charge in the UK.

Analysis and Conclusion

The specter of a “digital pearl harbor” at the hands of terrorists continues to shadow us but a massive campaign of destructive cyber terrorism has **not materialized to date**.

“Terrorist groups may use the Internet more to influence public perception and coordinate their activities. The internet is likely to have greater value to them when it is fully operational” (Denning, 1999, p. 71).

Current research and literature survey for this paper indicate that an **immediate threat from cyber terrorism has a low probability**.

Analysis and Conclusion

“ People are more afraid of the physical carnage from terrorists’ bombs and bullets than a blank computer screen! “ Rick Forno, Security Consultant

Sources

Alshech, E. (2007, February 27). Cyberspace as a combat zone: The phenomenon of electronic jihad. Jerusalem Post.

Arquilla, J., & Ronfeldt, D. F. (1996). The advent of netwar. Santa Monica, CA: Rand.

Bongar, B., Brown, L. M., Beutler, L. E., Breckenridge, J. N., & Zimbardo, P. G. (2006). Psychology of terrorism (1st ed.). New York: Oxford University Press.Brachman, J. (2006, Summer). High tech terror.

Bunker, R., & Begert, M. (2005). Operational combat analysis of the Al Qaeda network. In R. Bunker (Ed.), networks, terrorism, and global insurgency (pp. p. 161). New York: Routledge.

Bunker, R., & Sullivan, J. (2005). Multilateral counter-insurgency networks. In R. Bunker (Ed.), Networks, terrorism, and global insurgency (pp. pp.183-197). New York: Routledge.

Cilluffo, F., & Saathoff, G. (2007). Networked radicalization: Counter-strategy.

Denning, D. (2007). A view of cyberterrorism five years later. In K. Himma (Ed.), Internet security: hacking, counterhacking, and society. Sudbury, MA: Jones and Bartlett Publishers.

Denning, D. D. (1999). Information warfare and security. New York: ACM Press Books.

Denning, D. E., & Baugh, W. E. (1997, January 23). Cases involving encryption in crime and terrorism.

Ehrenfeld, R., & Wood, J. (2007, May 23). Outside view: Terror, crime go digital.

Forno, R., & Baklarz, R. (1999). The art of information warfare (2nd ed.). Boca Raton, FL: Universal Publishers.

Alshech, E. (2007

Sources

Gartenstein-Ross, D., & Dabruzzi, K. (2007). The convergence of crime and terror: law enforcement opportunities and perils. : Center for Policing Terror.

Geostrategy-Direct (2007, July 18). Focus on terrorism: Week of July 18, 2007.

Granger, S. (2001, December 18). Social engineering fundamentals, part I: Hacker tactics.

Haussler, N. I. (2005, Third generation gangs revisited: The Iraq insurgency September 2005). Third generations gangs revisited: The IRAQ insurgency.

Hoffman, B. (2006). Inside terrorism (revised and expanded ed.). New York: Columbia University Press.

IntelCenter (2007, June). Jihadi tactics and targeting statistics.

James Foundation (2007, June). Forum users improve electronic jihad technology. Terrorism Focus, IV, 20,

Krebs, B. (2007, July 5). Brian Krebs on computer security.

Krebs, B. (2007, July 5). Terrorism's hook into your inbox.

Marsellla, A. J. (2004). Reflections on international terrorism: Issues, concepts, and directions. In F. M. Moghaddam, & A. J. Marsella (Eds.), Understanding terrorism: Psychological roots, consequences, and interventions (pp. p. 16). Washington, DC: American Psychological Association.

Reuters (2007, June 22). US general laments Google Earth capability.

Robb, J. (2007). Brave new war: The next stage of terrorism and the end of globalization. Hoboken, New Jersey: John Wiley & Sons, Inc.

Sources

Rollins, J., & Wilson, C. (2005, October 20). Terrorist capabilities for cyberattacks: overview and policy issues Congressional Research Service Report for Congress, p. 17.

Ronfeldt, D., & Arquilla, J. (2001). What Next for Networks and Netwars?" in J. Arquilla, & J. Ronfeldt (Eds.), Networks and netwars: The future of terror, crime, and militancy (pp. 322-325). Sanata Monica, CA: Rand.

Sandia National Laboratories (2002, November 21). Terrorist organizations and criminal street gangs. Senate Committee on Homeland Security & Governmental Affairs (2007, May 03). Terrorists' uses of the Internet to recruit, train, and launch attacks.

Sullivan, J. (2005). Terrorism, crime, and private armies. In R. Bunker (Ed.), Networks, terrorism, and global insurgency (pp. pp. 69-83). New York: Routledge.

Talbot, D. (2005, January 27). Terror's server - How radical Islamists use Internet fraud to finance terrorism and exploit the Internet for Jihad propaganda and recruitment.

The Jamestown Foundation (2007, March 29). The new issue of technical mujahid, a training manual for jihadis.

Weimann, G. (2006). Terror on the Internet (1st ed.). Washington, DC: Unites States Institute Of Peace Press.

Zanini, M., & Edwards, S. (2001). Networking of terror in the information age in J. Arquilla, & D. F. Ronfeldt (Eds.) Networks and netwars: The future of terror, crime, and militancy (pp. 29-60). Santa Monica, CA: Rand.

US Fed News (2007, May 18). Terrorist on the Internet. US Fed News