The Myth of Cyber-Terrorism

Why bin Laden != `/bin/laden`

> ***"Terrorism is like lightning. It takes the path of least resistance to its end. And, right now, it's easier to blow something up than to figure out how to damage it by hacking into and manipulating a computer system."***
>
> ***-- Scott Berinato***

What Terrorism Is…and Isn't

- Competing definitions of "terrorism"
  - "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." -- FBI
  - "Premeditated, politically-motivated violence perpetrated against noncombatant targets by sub-national groups or clandestine agents, usually intended to influence an audience." -- U.S.C., Title 22, Ch. 38, Sec. 2656f(d)

What Terrorism Is…and Isn't

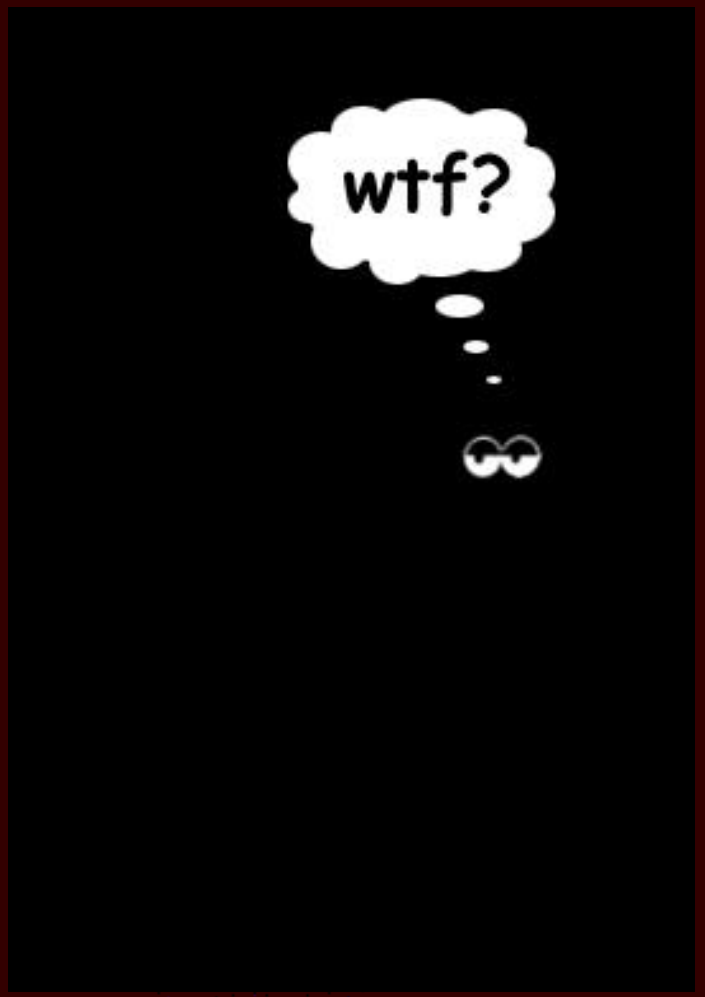
- Major hallmarks of terrorism
  - Real, imminent threat of death or dismemberment
  - Psychological impact of attack
  - Destruction of faith or trust
  - Long-term consequences
  - Most importantly, terrorism instills a sense of mortal terror in the survivors

What Terrorism Is…and Isn't

- Comparison of psychological impact:
  - 9/11/2001: Everyone remembers the moments precisely. Experience is frozen in time (like JFK's assassination & Challenger explosion)
  - 9/18/2001: Ask the average citizen what happened on that date. The vast majority have no recollection whatsoever. (Even if they were IIS admins…)
  - Other major net.incidents accorded equal lack of impact. (11/2/1988, for example)

What Terrorism Is…and Isn't

Comparison of psychological impact: WTC vs. WTF



What Terrorism Is…and Isn't

- Weapons of Mass Distraction
  - Two flavors of predicted "cyber-terrorism":
    - Physical infrastructure threat (power, water, phones, hospitals, air traffic control)
    - Critical data threat (theft, subversion of info, or irreversible destruction of vital data)
  - Both scenarios predict thousands dead.
    - Meaningless. 40,000+ die each year due to a correctly-functioning technology; the car.
    - Under critical review, cyber-terrorism scenarios don't really involve death, but inconvenience.

What Terrorism Is…and Isn't

- Weapons of Mass Distraction (con't)
  - Even those who claim to take cyber-terrorism seriously betray genuine beliefs by chronic inaction. (Psych: "La belle indifference.")
    - 1996: Clinton convened panel of experts
    - 1997: Panel released its unremarkable findings
    - 1998: Pentagon - 30 crackers with $10M could take U.S. down. Gartner claims 5 and $50M.
    - 2000: Nat'l Plan for Info Systems Protection.
    - 2002: National Strategy to Secure Cyberspace.
    - Recurring theme: *"It will affect the man in Iowa."*

What Terrorism Is…and Isn't

- Weapons of Mass Distraction (con't)
  - Scary scenarios in which the power and phones are knocked out.
    - California government has been doing a fine job of that all by itself for the past few years.
    - AT&T did an unparalleled job of DoS'ing themselves to oblivion in January 1990.
    - Americans have been through floods, fires, riots, hurricanes, earthquakes, and (in the past decade) major terrorist attacks, all of which knocked out many major utilities, and we've fared just fine.

What Terrorism Is…and Isn't

- Weapons of Mass Distraction (con't)
  - It's now several years later. In spite of all this FUD-mongering, has anything changed for the better?
    - Worms still abound; Slapper being the latest.
    - Public systems still 0wn3d by scriptkiddies.
  - Even William Church, Intelligence Analyst with the Center for Infrastructural Warfare Studies admits: "Terrorists aren't quite ready for infowar."

Terrorist Tempest in a Teapot

"The information-war people say this cyber-terrorist threat is out there, but they never provide any plausible scenarios. I'm asking for reality, and I'm not getting it."

-- Rob Rosenberger, Vmyths.com

Terrorist Tempest in a Teapot

- Modus Operandi: Keep It Simple, Sirrah
  - Terrorists don't experiment with (or trust) new or unfamiliar technologies.
  - Terrorist arsenals proliferate from states long after the weapons are proven in combat.
  - Unconventional use of low-tech & old-tech.
    - Why build an elaborate delivery vehicle when you can use homicide bombers?
    - Their “guided missiles” on 9/11 were conventional aircraft with suicide pilots.
    - USS Cole attack: “torpedo” was bomb-laden boat.

Terrorist Tempest in a Teapot

- Modus Operandi: Keep It Simple… **(con't)**
  - Irish Republican Army
    - Had computer-oriented cells.
    - Those cells were capable of infowar.
    - Yet the IRA preferred physical weapons.
  - Sri Lankan "Tamil Tigers"
    - Their "cyber-terror" was e-mail bombardment.
    - That's not terrorism, that's spam.

Terrorist Tempest in a Teapot

- Modus Operandi: Keep It Simple… **(con't)**
  - Terrorists do not rely on sophisticated attacks.
    - Cyber warfare is incredibly sophisticated.
    - Attacker has to know the technology and how to exploit it.
    - Attacker has to possess the technology (whether owned or 0wn3d).
  - Even those capable of such concerted attack aren't motivated by ideology, but personal gain.

Terrorist Tempest in a Teapot

- Modus Operandi: Keep It Simple… **(con't)**
  - Our foe is notoriously anti-Western
    - Terrorists do not recruit outside their own fanatical circles. Their foot-soldiers are those who've abandoned the West and are anti-technology.
    - This precludes courting of skilled intruders. (Not likely to dump high-tech life of convenience to eat dirt in some backwater nation.)
    - Terrorists won't gamble on hacker's loyalty. (Why take a job for a mere $250K when you can cash in for $5 million via Rewards for Justice Fund?)

Terrorist Tempest in a Teapot

- In professing themselves wise, they exposed themselves as fools. (Painful ignorance of high-tech weaponry.)
  - Much-hyped fission bomb plans
    - Found in Afghanistan cave.
    - It was a humor document for sale on the Web.
  - Red Mercury
    - Multiple terrorist orgs *still* trying to purchase it.
    - One problem: it exists only in fables of alchemy.
    - Only confirmed use was in name alone...in arms trafficking sting years ago.

Terrorist Tempest in a Teapot

- The Big Picture
  - Even incidents involving disrupted utilities & air traffic lacked hostile intent.
    ("Oops." != "Jihad!")
  - Utility failures don't evoke any sense of fear, they evoke annoyance.
  - Most importantly, terrorists are bound to stark visual impressions…

Sensitive people should avert their eyes now.

Terrorist Tempest in a Teapot

- ***This*** is terrorism.

We Have Met the Enemy...

"Most of the time I feel like I'm watching a really bad cartoon."

-- John Pike, defense analyst for the Federation of American Scientists

We Have Met the Enemy...

- Recap: FBI definition of terrorism
  - Using force to intimidate or coerce government or civilians to further an agenda.
  - Cyber-terrorism therefore defined as the use of computing resources to intimidate or coerce others.
  - It makes more sense to classify Microsoft, the MPAA, RIAA, and the DMCA as cyber-terrorists rather than any al Qaeda cracker.

We Have Met the Enemy...

- Fast, Furious and Futile…
  - 9/12/2001: NIPC had an emergency meeting to collect & analyze cyber-intelligence info.
    - Wonderful public relations gimmick.
    - Didn't predict, prevent, or even blunt the impact of Nimda, which occurred a mere six days later.
  - Patriot Act amended electronic surveillance laws. Tougher penalties for hacking.
    - Only discourages casual digital joy riders.
    - Terrorists don’t care; they don’t trust electronic communication; and death wishes are their ***hobby***.

We Have Met the Enemy...

- Slow, Stupid and Superfluous...
  - Elizabeth Parker, former General Counsel for CIA & NSA claims we're vulnerable because cyber-defense "is not well understood and is not talked about sufficiently."
    - It's talked about. It's been talked into the ground for the better part of a decade!
    - We've even got the recipe: RFC 2196!
  - But nothing is ***done***.

We Have Met the Enemy...

- Asleep at the Switch
  - Incidents that could have been terrorist attack could have been easily detected & prevented.
    - 1997: Worcester, MA airport control tower shut down. (The airport wasn't the target; NYNEX loop carrier systems were.)
    - 2000: Australian waste management control system tricked into dumping millions of gallons of raw sewage. (Attacker made 46 separate attempts to do his dirty deed. Nobody noticed the first 45.)
  - All courtesy of indifference to basic security.

We Have Met the Enemy...

- Stranger than Fiction
  - All manner of media hype.
    - If it's not pedophiles on the Internet, it's terrorists.
    - 2002: USA Today claimed al Qaeda sending hundreds of encrypted messages in images hidden on eBay and other public web sites.
    - Neils Provos and others have been trying to verify this claim without success. They've been crawling the 'net and have analyzed over 2,000,000 images. ***They have yet to find even <u>one</u> image with steganographic content.***

We Have Met the Enemy...

- The Incredibly Big & Scary Nothing
  - Even the oft-claimed cyber-attack on our air traffic system is overblown.
    - Scenario requires taking all humans out of the loop and negating all rules of the air.
    - Pilots routinely catch errors committed by air traffic controllers. (Every air disaster occurs from *multiple* failures; even July 1 collision between Russian Tupolev & Boeing 757.)
    - Finally, rules of the air ***are based on total failure of air traffic control.***

We Have Met the Enemy...

- The Incredibly Big & Scary Nothing (con't)
  - The much-hyped subversion of information
    - In 1996, Barry Collin speculated that a cyber-terrorist could take over cereal manufacturing process control system and poison children by increasing the iron supplement dosage.
    - This actually happened in the 1970s, but by accident.
    - Nobody died because the corn flakes looked "dirty" (you could ***see*** the flakes of iron) and the product tasted so foul that it was inedible.

We Have Met the Enemy...

- The Incredibly Big & Scary Nothing (con't)
  - Mouse that Roared vs. The Rat that Yawned.
    - The Mouse Mythos:
      - 1950s comedy: small nation attacks U.S. in hopes of being defeated so they can get loads of U.S. aid.
      - Everyone hunkered down in bunkers, so the invaders end up winning the "war."
    - The Rat Reality:
      - 19th century: ore miners paid close attention to the mine rats. Any sign of anxiety by the rats was sure indicator of impending disaster.
      - 21st century: Look at the hacking community. Nobody in the know (who isn't selling something) is panicking.

We Have Met the Enemy...

- Pound of Cure > Ounce of Prevention?
  - Politicians aren't helping with their antics.
    - Rep. Lamar Smith (R-TX) claims 50% chance that next hit will be cyber-attack.
      - Claims billions of dollars in losses and thousands dead.
      - Nevermind that previous non-terrorist hits such as Melissa & ILoveYou were reported to have claimed billions in losses as well. (Were those "losses" reported to stockholders? Hmmm.)
    - Even Chuck Schumer of New York is on the cyber-terror bandwagon, claiming imminent destruction of nation's utilities, air traffic control and nuclear power plants.

We Have Met the Enemy...

- Pound of Cure > Ounce of Prevention? (con't)
  - Politicians aren't helping with their antics. (con't)
    - Won't mandate minimum security requirements for vendors, but will pass more draconian laws against hackers and hacking tools & techniques.
    - DMCA criminalized reverse engineering, but who seriously thinks the terrorists care?
    - It's sad commentary when an admitted traitor who took up arms against U.S. (Taliban John) gets only 20 years, but making a monkey out of an online business can get you possible Life imprisonment.

We Have Met the Enemy...

- The *Real* Threat: The Axis of Inanity
  - Those who are responsible are not held accountable and vice-versa.
    - Vendors still absolve selves for putting us at risk.
    - Admins still not taken to task for not keeping up on security patches and workarounds.
    - Users still held blameless for their conduct.
    - Security staff still held to grim double standard ("We didn't get breached; we're cutting your budget." / "We got breached; you're useless.")
    - Full disclosure and unorthodox, legitimate security research demonized & stifled.

We Have Met the Enemy...

- The *Real* Threat: The Axis of Inanity (con't)
  - The hype doesn't help, it hurts!
    - Alarmist nonsense engenders learned helplessness.
    - Self-fulfilling prophecy.
    - Meaningful solutions ignored in the belief that they won't stop "cyber-terrorism."
    - National Security becomes just another marketing ploy, as is the case in Microsoft vs. Open Source.
    - Info on the 'net gets dumbed-down (though still readily available via public libraries). Absolutely ***no*** security benefit!

We Have Met the Enemy...

- Put Up or Shut Up
  - Infowar is better suited to espionage.
    - Quiet, difficult to detect, and non-lethal.
    - Terrorism is the antithesis of those qualities.
  - All this hype only trivializes the stark horror that is genuine terrorism.
  - The solutions already exist. It's the prevailing political priorities and commercial self-interests that are out of step with reality.
  - Know your enemy: your *real* enemy.

We Have Met the Enemy...

- And finally...

"If you spend more on coffee than you spend on IT security, then you will be hacked. What's more, you <u>deserve</u> to be hacked."

-- Richard Clarke,
Special Advisor to the President
on Cyberspace Security

Related Links

- **Latest edition of this presentation**
  http://www.treachery.net/~jdyson/toorcon2002/
- **Vmyths: Truth About Computer Virus Myths & Hoaxes**
  http://www.vmyths.com/
- **Debunking the Threat to Water Utilities**
  http://www.cio.com/archive/031502/truth_sidebar2.html
- **Detecting Steganographic Content on the Internet**
  http://www.citi.umich.edu/u/provos/stego/
- **Full story of the "FAA Control Tower Hacker"**
  http://www.usdoj.gov/criminal/cybercrime/juvenilepld.htm
- **InfoWarrior.Org: Spreading Sanity, Sharing Wisdom**
  http://www.infowarrior.org/
- **9-11 Justice.Org: Action for Justice, Not Appeasement**
  http://www.9-11justice.org/

About the Author

Jay D. Dyson is a Senior Security Engineer for the National Aeronautics and Space Administration's Jet Propulsion Laboratory. He is also founder and maintainer of Treachery Unlimited. His works include Early Bird (a realtime HTTP worm intrusion attempt notification utility), and his writings have been featured in SecurityFocus and SunWorld. He was also a contributing author to *Hack-Proofing Your Web Applications*. Mr. Dyson spends his free time collecting viruses, trojans & worms, and caring for his pet rats.

His current motto:

"Your security is not a joke.
Well...okay, it is."