doi :10.1145/1897816.1897829
communications of the acm | february 2011 | vol. 54 | no. 2 | pp.s 26 - 28

Viewpoints: Privacy & Security

Against Cyberterrorism

Why cyber-based terrorist attacks are unlikely to occur

Like the 2007 cyber attacks on Estonia, the October 2010 Stuxnet botnet attack on Iranian nuclear facilities made cyber-based attacks global news. The Estonian attacks were largely labeled a cyberwar by journalists, although some did invoke the concept of cyberterrorism. The Stuxnet attack, on the other hand, has been very widely described as cyberterrorism, including by the Iranian government.

Cyberterrorism is a concept that appears recurrently in contemporary media. It is not just reported upon in newspapers and on television, but is also the subject of movies (such as 1990's *Die Hard II* and 2007's *Die Hard IV: Live Free or Die Hard*) and popular fiction books (for example, Winn Schwartau's 2002 novel *Pearl Harbor Dot Com*). This coverage is particularly interesting if one believes, as I do, that no act of cyberterrorism has ever yet occurred and is unlikely to at any time in the near future. Having said that, it is almost always portrayed in the press as either having already occurred or being just around the corner. As an academic, I'm not alone in arguing that no act of cyberterrorism has yet occurred and, indeed, some journalists agree; most, however, seem convinced as to the salience of this threat. Why?

I can only surmise that, just as a large amount of social psychological research has shown, the uncertain and the unknown generally produce fear and anxiety. This is the psychological basis of an effective movie thriller: the fear is greatest when you suspect something, but you're not certain what it is. The term "cyberterrorism" unites two significant modern fears: fear of technology and fear of terrorism. Fear of terrorism, though the likelihood of any one of us being the victim of terrorism is statistically insignificant, has become perhaps normalized; but fear of technology? In fact, for those unfamiliar with the workings of complex technologies, these are perceived as arcane, unknowable, abstract, and yet increasingly powerful and ubiquitous. Many people therefore fear that technology will become the master and humankind the servant. Couple this relatively new anxiety with age-old fears associated with apparently random violence and the result is a truly heightened state of alarm. Many journalists—although fewer technology journalists than others— have succumbed, like members of the general population, to these fears, to which the journalists have then added further fuel with their reporting.

The Definition Issue

The second stumbling block for journalists is that just as the definition of terrorism is fraught, so too is the definition of cyberterrorism. My preference is to distinguish between cyberterrorism and terrorist use of the Net. This is the distinction FBI Director Robert Mueller seemed implicitly to be drawing in a March 2010 speech in which he stated that “the Internet is not only used to plan and execute attacks; it is a target in and of itself…We in the FBI, with our partners in the intelligence community, believe the cyber terrorism threat is real, and it is rapidly expanding.”[a] Where the FBI Director and I diverge is in the efficacy of the cyberterrorist threat as opposed to that of everyday terrorist use of the Net (that is, for radicalization, researching and planning, financing, and other purposes).

Dorothy Denning’s definitions of cyberterrorism are probably the most well known and respected. Her most recent attempt at defining cyberterrorism is: “…[H]ighly 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. It is the convergence of terrorism with cyberspace, where cyberspace becomes the means of conducting the terrorist act. Rather than committing acts of violence against persons or physical property, the cyberterrorist commits acts of destruction or disruption against digital property.”(2)

Analyses of cyberterrorism can be divided into two broad categories on the basis of where the producers stand on the definition issue: those who agree broadly with Denning versus those who wish to incorporate not just use, but a host of other activities into the definition. The literature can also be divided on the basis of where the authors stand on the magnitude of the cyberterrorism threat. Dunn-Cavelty uses the term “Hypers” to describe those who believe a cyberterrorist attack is not just likely, but imminent,[b] and the term “De-Hypers” to describe those who believe such an attack is unlikely.(1) Most journalists are hypers, on the other hand I’m emphatically a de-hyper. In this column, I lay out the three major reasons why.

Three Arguments Against Cyberterrorism

In my opinion, the three most compelling arguments against cyberterrorism are:

- The argument of Technological Complexity;
- The argument regarding 9/11 and the Image Factor; and
- The argument regarding 9/11 and the Accident Issue.

The first argument is treated in the academic literature; the second and third arguments are not, but ought to be. None of these are angles to which journalists appear to have devoted a lot of thought or given adequate consideration.

In the speech mentioned earlier, FBI Director Mueller observed “Terrorists have shown a clear interest in pursuing hacking skills. And they will either train their own recruits or hire outsiders, with an eye toward combining physical attacks with cyber attacks.” That may very well be true, but the argument from Technological Complexity underlines that ‘wanting’ to do something is quite different from having the ability to do the same. Here’s why:

Violent jihadis’ IT knowledge is not superior. For example, in research carried out in 2007, it was found that of a random sampling of 404 members of violent Islamist groups, 196 (48.5%) had a higher education, with information about subject areas available for 178 individuals. Of these 178, some 8 (4.5%) had trained in computing,

[a] The text of Director Mueller’s March 2010 speech at a cyber security conference in San Francisco is available at http://www.fbi.gov/pressrel/speeches/mueller030410.htm.

[b] See, for an exemplary example, journalist Dan Verton’s *Black Ice: The Invisible Threat of Cyberterrorism*. McGraw-Hill, New York, 2003.

which means that out of the entire sample, less than 2% of the jihadis came from a computing background.(3) And not even these few could be assumed to have mastery of the complex systems necessary to carry out a successful cyberterrorist attack.

Real-world attacks are difficult enough. What are often viewed as relatively unsophisticated real-world attacks undertaken by highly educated individuals are routinely unsuccessful. One only has to consider the failed car bomb attacks planned and carried out by medical doctors in central London and at Glasgow airport in June 2007.

Hiring hackers would compromise operational security. The only remaining option is to retain "outsiders" to undertake such an attack. This is very operationally risky. It would force the terrorists to operate outside their own circles and thus leave them ripe for infiltration. Even if they successfully got in contact with "real" hackers, they would be in no position to gauge their competency accurately; they would simply have to trust in same. This would be very risky.

So on the basis of technical knowhow alone cyberterror attack is not imminent, but this is not the only factor one must take into account. The events of Sept. 11, 2001 underscore that for a true terrorist event spectacular moving images are crucial. The attacks on the World Trade Center were a fantastic piece of performance violence; look back on any recent roundup of the decade and mention of 9/11 will not just be prominent, but pictures will always be provided.

The problem with respect to cyberterrorism is that many of the attack scenarios put forward, from shutting down the electric power grid to contaminating a major water supply, fail on this account: they are unlikely to have easily captured, spectacular (live, moving) images associated with them, something we—as an audience—have been primed for by the attack on the World Trade Center on 9/11.

The only cyberterrorism scenario that would fall into this category is interfering with air traffic control systems to crash planes, but haven't we seen that planes can much more easily be employed in spectacular"real-world" terrorism? And besides, aren't all the infrastructures just mentioned much easier and more spectacular to simply blow up? It doesn't end there, however. For me, the third argument against cyberterrorism is perhaps the most compelling; yet it is very rarely mentioned.

In 2004, Howard Schmidt, former White House Cybersecurity Coordinator, remarked to the U.S. Senate Committee on the Judiciary regarding Nimda and Code Red that "we to this day don't know the source of that. It could have very easily been a terrorist."(4) This observation betrays a fundamental misunderstanding of the nature and purposes of terrorism, particularly its attention-getting and communicative functions.

A terrorist attack with the potential to be hidden, portrayed as an accident, or otherwise remain unknown is unlikely to be viewed positively by any terrorist group. In fact, one of the most important aspects of the 9/11 attacks in New York from the perpetrators viewpoint was surely the fact that while the first plane to crash into the World Trade Center could have been accidental, the appearance of the second plane confirmed the incident as a terrorist attack in real time. Moreover, the crash of the first plane ensured a large audience for the second plane as it hit the second tower.

Alternatively, think about the massive electric failure that took place in the northeastern U.S. in August 2003: if it was a terrorist attack—and I'm not suggesting that it was—but *if it was*, it would have been a spectacular failure.

Conclusion

Given the high cost—not just in terms of money, but also time, commitment, and effort—and the high possibility of failure on the basis of manpower issues, timing, and complexity of a potential cyberterrorist attack, the costs appear to me to still very largely outweigh the potential publicity benefits. The publicity aspect is crucial for potential perpetrators of terrorism and so the possibility that an attack may be apprehended or portrayed as an accident, which would be highly likely with regard to cyberterrorism, is detrimental. Add the lack of spectacular moving images and it is my belief that cyberterrorism, regardless of what you may read in newspapers, see on television, or obtain via other media sources, is not in our near future.

So why then the persistent treatment of cyberterrorism on the part of journalists? Well, in this instance, science fiction-type fears appear to trump rational calculation almost every time. And I haven't even begun to discuss how the media discourse has clearly influenced the pronouncements of policymakers.[c]

References

1. Cavelty, M.D. Cyber-Terror: Looming threat or phantom menace? The framing of the U.S. cyberthreat debate. *Journal of Information Technology and Politics 4*, 1 (2007).

2. Denning, D. A view of cyberterrorism five years later. In K. Himma, Ed., *Internet Security: Hacking, Counterhacking, and Society* (Jones and Bartlett Publishers, Sudbury, MA, 2006), 124.

3. Gambetta, D. and Hertog, S. Engineers of Jihad. *Sociology Working Papers, No. 2007–10*, Department of Sociology, University of Oxford, (2007), 8–12; http://www.nuff.ox.ac.uk/users/gambetta/Engineers%20of%20Jihad.pdf.

4. Virtual Threat, Real Terror: Cyberterrorism in the 21st Century (Serial No. J–108–58), hearing before the Subcommittee on Terrorism, Technology and Homeland Security of the Committee on the Judiciary, United States Senate, 108th Congress, Second Session, (Feb. 4, 2004), http://cip.gmu.edu/archive/157_S108VirtualThreathearings.pdf.

Maura Conway (maura.conway@dcu.ie) is Lecturer in International Security in the School of Law and Government at Dublin City University in Dublin, Ireland.

[c] For more on the issues relating to media coverage of cyberterrorism raised in this column, including analysis of the pronouncements of policymakers in this regard, see "Media, Fear and the Hyperreal: The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures." In M.D. Cavelty and K.S. Kristensen, Eds., *Securing "The Homeland": Critical Infrastructure, Risk and (In)Security* (Ashgate, London, 2008), 109-129.