Cyber-Security Threats, Information Warfare and Critical Infrastructure Protection

By

Dr. Lopamudra Bandyopadhyay

The systems and networks that make up the infrastructure of society are often taken for granted, yet a disruption to just one of those systems can have dire consequences across other sectors. An entire region can become debilitated because some critical elements in the infrastructure have become disabled through natural disaster. If the disaster is man made or a result of criminal or political conspiracy, then the dangers are far greater for a rather vulnerable modern society that is based on interlinked infrastructures and whose foundations are erected on the basis of a virtual network of command and control operations. This particular academic paper deals with the dangers that are posed by the attacks of both state and non state entities on cyber space and the critical infrastructures that are the essential foundations of any modern state.

A computer attack may be defined as actions directed against computer systems to disrupt equipment operations, change processing control, or corrupt stored data. Different attack methods target different vulnerabilities and involve different types of weapons. Three different methods of attack have been identified. However, as technology evolves, distinctions between these methods may begin to blur.[i]

- A physical attack involves conventional weapons directed against a computer facility or its transmission lines;
- An electronic attack (EA) involves the use of the power of electromagnetic energy as a weapon, more commonly known as an electromagnetic impulse (EMP) to overload computer circuitry, but also in a less violent form, to insert a stream of malicious digital code directly into enemy microwave radio transmission; and
- A computer network attack (CNA), usually involves malicious code used as a weapon to infect enemy computers to exploit a weakness in software, in the system configuration, or in the computer security practices of an organisation or computer user. Other forms of CNA are enabled when an attacker uses stolen information to enter restricted computer systems.[ii]

The computer age has opened up possibilities for terrorists and hostile governments that did not exist before. Just as it has brought about a revolution in military planning and preparation, it has given birth to information terrorism, or cyber terrorism, and the threat of information warfare.[iii]

There are many variants on the basic definition of ‘terrorism’. One example is as follows: Terrorism is the calculated and unlawful use of force or violence, or threat of force or violence, against persons or property to inculcate fear, intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of goals that are generally religious, political, or ideological.[iv]

Cyber terrorism adds an element to that definition. Cyber terrorism is the definition of terrorism with the addition, “through the exploitation of computerized systems deployed by the target.”[v] Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, coined the term ‘cyber terrorism’ in the 1980s. Cyberspace, according to Collin may be conceived as “that place in which computer programs function and data moves.”[vi]

Combining these definitions result in a narrowly drawn working definition of cyber terrorism: premeditated, politically motivated attacks by subnational groups or clandestine agents against information, computer systems, computer programmes, and data that result in violence against noncombatant targets. By this definition, sending pornographic emails to minors, posting offensive content on the Internet, defacing web pages, stealing credit card information, posting credit card numbers on the Internet, and clandestinely redirecting Internet traffic from one site to the other do not constitute instances of cyber terrorism.[vii]

According to Dorothy Denning,[viii] “Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean 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. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not."[ix]

Cyber terrorism is the use of computer network tools to harm or shut down critical national and international infrastructures. The premise of cyber terrorism is that as nations and critical infrastructure become more dependent on computer networks for their operation, new vulnerabilities are created – "a massive electronic Achilles' heel."[x] Cyber crime and cyber terrorism are not coterminous. Cyberspace attacks must have a 'terrorist' component to be labeled cyber terrorism. The attacks must instill terror as commonly understood, and they must have a political motivation. As for terrorist use of information technology and terrorism involving computer technology as a weapon/target, only the latter may be defined as cyber terrorism. Terrorists' 'use' of computers as a facilitator of their activities, whether for propaganda, communication, or other purposes, is simply that: 'use'. And the vast majority of terrorist activity on the Internet is limited to 'use.'

The Monterey group[xi] defined three levels of cyber terror capability:[xii]

- Simple-Unstructured: The capability to conduct basic hacking against individual systems using tools created by someone else. The organisation possesses little target analysis, command and control, or learning capability.
- Advanced-Structured: The capability to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools. The organisation possesses an elementary target analysis, command and control, and learning capability.

- Complex-Coordinated: The capability for coordinated attacks capable of causing mass-disruption against integrated, heterogeneous defences (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organisation learning capability.

They estimated that it would take a group starting from the basics, two to four years to reach the advanced-structured level and six to ten years to reach the complex-coordinated level, although some groups might get there in just a few years or turn to outsourcing or sponsorship to extend their capability.[xiii]

Critical Infrastructure Protection or CIP is a national programme to assure the security of vulnerable and interconnected infrastructures of the United States. On May 22, 1998, President Bill Clinton issued Presidential decision directive PDD-63 on the subject of Critical Infrastructure Protection.[xiv] This recognized certain parts of the national infrastructure as critical to the national and economic security of the United States and the well-being of its citizenry, and required steps to be taken to protect it. This was updated on December 17, 2003 by President Bush through Homeland Security Presidential Directive HSPD-7[xv] for Critical Infrastructure Identification, Prioritization, and Protection. The directive broadened the definition of infrastructure in accordance with the Patriot Act, as the physical and virtual systems that are ' so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety.'[xvi]

Precisely the term ‘catastrophic terrorism’ entered general use as a result of the fact that it is closely linked to CIP (critical infrastructure protection), which was always understood in terms of national security, because it was primarily in this context that it was developed. Ashton B. Carter and William J. Perry[xvii] were the first to mention the term in Carter's co-authored 1998 article in the Foreign Affairs,[xviii] as well as in their 1999 book called Preventive Defense: A New Security Strategy for America.[xix]

Indian Computer Emergency Response Team (CERT-In)

The department of IT (Govt. of India) in 2004 established the Indian Computer Emergency Response Team (CERT-In)[xx] to respond to computer security incidents reported by the Indian Cyber community. CERT-In provides reactive and proactive services for enhancing cyber security. Incident response teams with expertise on major hardware and software platforms have been set up to confront the security concerns.

The following are the roles and functions that have been assigned to the CERT – In[xxi]:

Roles

a) Reactive

1. Provide a single point of contact for reporting local problems.
2. Assist the organisational constituency and general computing community in preventing and handling computer security incidents.
3. Share information and lessons learned with CERT/CC, other CERTs, response teams, organisations and sites.
4. Incident Response.
5. Provide a 24 x 7 security service.

6. Offer recovery procedures.
7. Artifact analysis
8. Incident tracing

b) Proactive

1. Issue security guidelines, advisories and timely advice.
2. Vulnerability analysis and response
3. Risk Analysis
4. Security Product evaluation
5. Collaboration with vendors
6. National Repository of and a referral agency for, cyber-intrusions.
7. Profiling attackers.
8. Conduct training, research and development.
9. Interact with vendors and others at large to investigate and provide solutions for incidents.

Functions

a) Reporting

- Central point for reporting incidents
- Database of incidents

b) Analysis

- Analysis of trends and patterns of intruder activity
- Develop preventive strategies for the whole constituency

- In-depth look at an incident report or an incident activity to determine the scope, priority and threat of the incident.

c) Response

- Incident response is a process devoted to restoring affected systems to operation
- Send out recommendations for recovery from, and containment of damage caused by the incidents.
- Help the System Administrators take follow up action to prevent recurrence of similar incidents

However, a detailed perusal of CERT-In's functions as well as jurisdiction and a detailed study of the IT Act of 2000[xxii] on the basis of which India's cyber security mechanism stands, clearly illustrate the fact that not much has been done with regard to Critical Infrastructure Protection. Laws are there to combat cyber terrorism and cyber crime, but the importance of Critical Infrastructure Protection in the event of any such catastrophe seems to have been overlooked.

Tools of Terror

The main weapons in this new kind of warfare are computer viruses,[xxiii] programmed to damage software; logic bombs, set to detonate at a certain time and destroy or rewrite data; and HERF (high-energy radio frequency) guns that disable electronic targets through high power radio signals. A suitcase-size device can generate high-powered electromagnetic impulses affecting all electronic components in the vicinity. Computer viruses can shut down entire computer systems through self-replication on available disc space. There are logic bombs (hostile programmes clandestinely introduced into target computers), called trapdoors, Trojan horses, worms, and spy chips. And as technology develops, so does the number of possibilities to create havoc.[xxiv] The number of potential targets is almost endless and is bound to grow along with the growth of information systems. Thinking ambitiously, financial markets could be affected by the destruction of records and the introduction of false information. Electrical transformers and power grids could be shut down. Air traffic control could be tampered with, causing collisions and eventually closing down civilian air transport. Interfering with the electronic avionic systems of planes in the air could also cause crashes. Similarly tanks and surveillance aircraft, as well as satellites could be made to malfunction or even be destroyed by high-energy weapons, or on a more primitive level, by interfering with the production processes and formulae.[xxv]

The cyberterrorist’s traditional weapons of choice include computer viruses (such as logic bombs that wake up on a certain date, worms and Trojan horses), cracking (accessing computer systems illegally), sniffing (monitoring Internet traffic for passwords, credit card numbers and other data), social engineering (fooling people into revealing passwords and other information) and dumpster diving (sorting through the trash).[xxvi] One of the most heralded weapons of a cyberterrorist or a hacker is the computers virus. Computer viruses are programmes designed to perform actions not intended by the operator. These actions include erasing or modifying the data in a computer's memory or storage with or without malicious intent. A virus is so named because it "lives" within a host system or programme and cannot spread without some acting, often unwitting (such as using an infected disk), by the system operator.

(1) **Computer Viruses**: Viruses can be used in an attempt to shut down a computer or even hold it hostage. The front page publicity granted the Michelangelo virus every March serves as an example of the publicity power generated by hostile virus. This particular virus was written to check the computer's internal clock/calendar and destroy the data on the infected computer on Michelangelo's birthday, March 6. The virus was widely publicised when released in 1992. To compete against virus detection and removal programs, virus writers have created a subset of the virus, known as a polymorphic virus. This type of virus changes itself slightly every time it is replicated or executed, thus denying a virus detection programme a fixed set of ‘indicators’ that the virus has infected a computer. Once released, the virus can be studied to find a method to prevent its further spread and remove it form the system. The computer community is striving to regain the initiative by developing operating systems that are more resistant to viruses. Despite these developments, those that attack computer systems will generally hold the initiative.

(2**) Trojan Horses**: The second type of weapon is a Trojan horse. True to its name, it is a program that does not appear to be destructive but releases a second programme to perform a task unintended by the system operator. A Trojan horse can be used to install a password ‘sniffer’ programme that collects the passwords of valid users and stores them for later use by an intruder posing as a legitimate user. Cyberterrorists can utilise this type of weapon for espionage to gain the information needed to access a system by impersonating legitimate users, thus compounding the problem of intrusion detection.

(3) **Worms**: Worms are programmes originally developed to travel through systems and perform mundane tasks, such as data collection or ensure of old data. While they can be useful, if misprogrammed or programmed with malicious intent, they can be extraordinarily destructive. A virus attaches itself to a host programme, but a worm is designed to spread across a computer network independently. While normally programmed to perform a task on a network, a worm may also simply replicate itself on target computers while it continues to spread across a network.

(4) **Humans**: Computer operators are the vehicles by which viruses, Trojan horses, and worms are initially programmed and then inserted into computer systems. In addition to utilising software attacks on a computer system, a cyberterrorist or hacker can attack a computer system through the vulnerability of its operators. The hacker community commonly refers to this as “social engineering.” Using a social engineering tactic, a cyberterrorist may impersonate a computer technician and call individuals within the targeted organisation to obtain information to penetrate a system. Once in possession of legitimate log on information, cyberterrorists will have ‘legal’ access to a system and can insert viruses, Trojan horses, or worms to expand their control of the system or shut it down.

(5) **Electro-Magnetic Pulse Weapons**: While not nearly as widespread as viruses, there exists a class of weapons that destroy computers and electronics through an electromagnetic pulse. The capability now exists to generate an instantaneous electromagnetic pulse that will overload and destroy the sensitive circuitry in advanced electronics and computer systems without the previously required detonation of nuclear weapons in the upper atmosphere. Any system that is within the limited range of these weapons will be disrupted or have its electronic components destroyed.

In the same manner as a bomb can be assembled by a conventional terrorist, a cyberterrorist can manufacture an EMP/T bomb out of readily available electrical and electronic components. TEMPEST devices (Transient Electro-Magnetic Pulse Emanation Standard) pick up radiation mainly from monitors and connecting cables. They allow cyber spies to intercept password, proprietary business plan, or personal letters, clearly displayed on their monitors.

Recommendations and Conclusion

The following recommendations may be adhered to with regard to the security aspect as far as cyber space attack may be concerned:

a. The Indian government must establish a clear distinction between general cyber-crime and cyber-warfare.
b. Real vulnerabilities should be identified.
c. Define national governmental and private systems that are truly critical and ensure they are isolated from attack, emergency alternatives exist, and they can be rapidly reconstituted.
d. It needs to be understood that defense also involves offence.
e. It is unclear whether tools for online warfare exist, and extensive R & D efforts may be needed to improve them.
f. The Indian Govt. needs to develop a clear response doctrine.
g. India should reserve the right to respond unilaterally to attacks against its infrastructure.
h. Existing Domestic Law should be changed to reflect the reality of cyber–threats, cyber-warfare and CIP.

i. There must be a clear central point for handling of cyber-intelligence.
j. The issue of domestic intelligence gathering and surveillance needs to be revisited.
k. Finally, there must be a central organization that is trained and equipped to deal with the domestic component of cyber-warfare and responds to attacks by governments and terrorists.

In conclusion it may be stated that there are a great number of international and domestic cyber terrorists as well as hackers and virus writers employed by hostile governments who are capable of seriously damaging governmental and financial institutions. These groups and/or lone individuals will increasingly rely on cyber terrorism to accomplish their social and political goals because of the numerous advantages of cyber terrorism and the vulnerability of the modern critical infrastructures that are the backbone of any state. Although these cyber terrorists will attack, there are agencies on an international, central, and state and local level, which are developing counter cyber terrorism abilities. Furthermore, although expensive and difficult to implement, there are protective measures that private corporations can implement in order to protect themselves.

President Bush's National Security Advisor, Condoleezza Rice, noted in March 2001 that "it is a paradox of our times that the very technology that makes our economy so dynamic and our military forces so dominating also makes us more vulnerable." She warned, "Corrupt [the information] networks, and you disrupt this nation."[xxvii] As a result of these concerns, a complex and overlapping web of national, regional and multilateral initiatives have emerged.[xxviii]

A common theme behind these initiatives is the recognition of the inadequacy of existing state-centric policing and legislative structures to police international networks and the importance of ensuring that private networks are secured against disruption. One way of grouping these initiatives is to use the standard information security paradigm of deterrence, prevention, detection and reaction.[xxix]

End Notes

[i] Clay Wilson, *Computer Attack and Cyber terrorism: Vulnerabilities and Policy Issues for Congress*, Congress Research Service, The Library of Congress, Washington, DC., April 2005, p. 2.

[ii] *Ibid*, pp. 2 – 3. Jason Sherman, "Bracing for Modern Brands of Warfare," *Air Force Times*, September 27, 2004, accessed electronically at http://www.airforcetimes.com/story.php?=1-AIRPAPER-358727.php

[iii] Helen Nissenbaum, "Hackers and the Battle for Cyberspace", *Dissent*, New York, Fall 2002, pp. 50 – 57.

[iv] Refer to the FBI Web Site accessed electronically at http://www.fbi.gov

[v] Barry C. Collin, *Cyber terrorism From Virtual Darkness: New Weapons in a Timeless Battle*, accessed electronically at http://www.counterterrorism.org

[vi] Maura Conway, "What is Cyber terrorism?" *Current History*, Philadelphia, Vol. 101, No. 659, December 2003, p. 436.

[vii] Ibid.

[viii] Dorothy E. Denning is Professor of Computer Science at Georgetown University. She has been working on cyberspace security issues and technologies for almost thirty years and is author of *Information Warfare and Security* and numerous other books and articles.

[ix] Dorothy E. Denning, *Cyber terrorism*, Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives, May 23, 2000, accessed electronically at http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

[x] J. Lewis, *Assessing the Risks of Cyber terrorism. Cyber War, and Other Cyber Threats*, Report submitted to the Center for Strategic and International Studies (CSIS), Washington, D.C., 2002, p. 1.

[xi] The Monterey Group is a think tank situated in California. The organisation's web site is at http://cns.miis.edu

[xii] Denning, *op. cit.*

[xiii] *Ibid.*

[xiv] Document accessed electronically at http://fas.org/irp/offdocs/pdd-63.htm

[xv] Document accessed electronically at http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html

[xvi] *Ibid.*

[xvii] William J. Perry, U.S. Secretary of Defense from 1994 to 1997, is a senior fellow at the Hoover Institution. He is also the Michael and Barbara Berberian Professor at Stanford University, with a joint appointment in the Department of Engineering–Economic Systems/Operations Research and the Institute for International Studies. Ashton B. Carter was the Assistant U.S. Secretary of Defense for international security policy from 1993 to 1996 and is the Ford Foundation Professor of Science and International Affairs at the John F. Kennedy School of Government at Harvard University.

[xviii] Ashton Carter, John Deutch, and Philip Zelikow, "Catastrophic Terrorism: Tackling the New Danger," *Foreign Affairs*, New York, Vol. 77, No. 6, November/December 1998, pp. 80 – 94.

[xix] Ashton B. Carter and William J. Perry, *Preventive Defense: A New Security Strategy for America*, Brookings Institution Press, Washington, DC, 1999.

[xx] Refer to the Indian Computer Emergency Response Team (CERT-In) at http://www.cert-in.org.in

[xxi] *Ibid*, accessed electronically at http://www.cert-in.org.in/roles.htm

[xxii] Refer to the document of the bill at www.mit.gov.in/download/itbill2000.pdf

[xxiii] Marshall Brain, *How Computer Viruses and Worms Work*, accessed electronically at http://www.howstuffworks.com

[xxiv] Timothy W. Maier, "Is U.S. Ready for Cyberwarfare?", *Insight on the News*, New York, Vol. 15, No. 13, April 5 -12, 1999, p. 18.

[xxv] John Arquilla, David Ronfeldt and Michele Zanini, "Information-Age Terrorism," *Current History*, Philadelphia, Vol. 99, No. 636, April 2000, pp. 179 – 185.

[xxvi] All these terms are primarily information technology specific terms, or computer jargon.

[xxvii] Refer to http://www.state.gov

[xxviii] An overview of such activities is included in Andrew Rathmell and Kevin O'Brien (eds.), *Information Operations: A Global Perspective*, Jane's Information Group, Coulsden, 2000.

[xxix] Kevin A. O'Brien, "Networks, Netwar and Information-Age Terrorism," in Andrew Tan and Kumar Ramakrishna (eds.), *The New Terrorism: Anatomy, Trends and Counter-Strategies*, Eastern University Press, Singapore, 2002.