Cyberterrorism: A Tool of Asymmetric Warfare

Lieutenant Colonel Vikrant Lakhanpal

Historically, the world has been faced with a variety of threats: dictatorial rulers, colonialism, racial tensions, civil war, world war, cold war, segregation, terrorism, viral epidemics, depressions, and computer related problems. These threats have often received widespread public and media attention while in their "prime." However, the emergence of the "computer age" has spawned a mutation of an already familiar and much feared threat. Computers may revolutionise terrorism in the same manner that they have revolutionised everyday life.

Cyberterrorism

In the 1980s, Barry Collin[1], a senior research fellow at the Institute for Security and Intelligence in California, coined the term "Cyberterrorism" to refer to the convergence of cyberspace and terrorism.[2]

The advent of cyberterrorism has forced a shift in the definition of terrorism to include both disruption and violence in cyberspace in the same manner as physical destruction and violence. Through the use of new technology, terrorist groups may have fewer members, yet have a global reach. The increasing power of computers may lower the threshold of state sponsorship to a point where poor states can become sponsors. The federal government of the USA has taken heed of this new threat, evidenced by the proposals from both the President and the Congress. The Department of Homeland Security alongwith a cyber security division was created by a legislation post 11 September 2001 incident. The federal government requested $4.5 billion for infrastructure security.[3] The FBI now boasts of more than one thousand "cyber investigators. It is evident that there is a growing concern in the USA about cyberterrorism at all levels.

Cyberterrorism and Modern Terrorist

Cyberterrorism is an attractive option for modern terrorists, who value its anonymity, potential to inflict massive damage,

---

Lieutenant Colonel Vikrant Lakhanpal is from 2 Mountain Division, Signals Regiment.

Journal of the United Service Institution of India, Vol. CXXXVI, No. 565, July-September 2006.

psychological impact, and media appeal. This enables them to carry out acts of terrorism from their own tent, cave, bunker, or palace. Other considerations are as under:-[4]

(a) Low cost.

(b) Large variety of targets.

(c) Low risk to terrorists.

(d) Greater media coverage.

Over a period of time, the level of sophistication required to hack into an information system has decreased. At the same time, the quality, quantity, and availability of hacking tools has increased. Cyber warrior tools are often readily available for downloading from the Internet. A comparatively low technology adversary with minimal funding, training, manning, and defence infrastructure can resort to cyberterrorism at short notice from anywhere in the world. This creates a very dangerous target-rich and low-risk combination.

Levels of Cyberterror Capability

In August 1999, the Center for Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey, California, conducted a study to assess the prospects of terrorist organisations pursuing cyberterrorism.[5] They defined the following three levels of cyberterror capability:-

(a) **Simple-Unstructured.** The capability to conduct basic hacks against individual systems using tools created by someone else. The organisation possesses little target analysis, command and control, or learning capability.

(b) **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.

(c) **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.

Motives

Physical attack is the simplest but the element of risk in execution is high. Nuclear, chemical, and biological attacks require sophistication of skills, knowledge, and materials and are more difficult to implement. In an asymmetric world, terrorists will look for alternate methods to spread terror. The cyber world may prove to be the simplest and quickest alternative to traditional physical attacks. Motives of cyber attacks may vary greatly such as – intimidation, coercion, retaliation, influence, power, specific objective, revenge, induce fear or panic, decrease public confidence in infrastructure, spread ideology (religious and/or political), or financial gain by cyberextortion.[6] The dilemma in the cyber world is not only to detect who is attacking (individual, group, or nation) but also understand the motive.

After the 11 Sepembter 2001 attacks on the US, security in general and cyberterrorism in particular featured prominently. This was understandable, given that more nightmarish attacks were expected and that cyberterrorism seemed to offer Al Qaeda opportunities to inflict enormous damage. But there was also a political dimension to the new focus on cyberterrorism. Combating cyberterrorism has become not only a highly politicised issue but also an economically rewarding one.[7] An entire industry has emerged to grapple with the threat of cyberterrorism. Think tanks have launched elaborate projects and issued alarming white papers on the subject. Experts have testified to cyberterrorism's dangers, and private companies have hastily deployed security consultants and software designed to protect public and private targets. Evidencing the US government's dedication to protection against cyberterrorism, the US Congress established a loan guarantee programme giving up to $10,000,000 to qualified borrowers. Under this programme, the government will fund the establishment for cyberterrorism prevention in order to meet the national security objectives. Besides the lobby looking at financial and political gains, the threat of cyberterrorism has been used to justify increased surveillance; and critics argue that it is merely an excuse to violate privacy rights. In fact, some activists claim the entire dialogue surrounding the issue of cyber-terror has been hyped out of proportion to the real threat, as a way to erode civil liberties, and give more draconian powers to the administration particularly in the United States. Also, hyping cyberterrorism makes eye catching

and intriguing news to the advantage of the media and dramatic potential for the novelists.[8]

Neither Al Qaeda nor any other terrorist organisation appears to have tried to stage a serious cyber attack. For now, the most damaging attacks and intrusions, experts say, are typically carried out either by disgruntled planted insiders intent on embezzlement or sabotage or by individual hackers seeking thrills and notoriety.[9] Jim Lewis, a sixteen-year veteran of the State and Commerce Departments, in a report for the Center for Strategic and International Studies titled "Assessing the Risks of Cyberterrorism, Cyber War, and Other Cyber Threats", mentions "The idea that hackers are going to bring the nation to its knees is too far-fetched a scenario to be taken seriously." Lewis argues that Nations are more robust than the early analysts of cyberterrorism and cyberwarfare give them credit for.

Osama Bin Laden has suggested that he has the expertise to use the computer as a weapon.[10] Bin Laden was quoted by the Ausaf newspaper after the 11 September 2001 attacks, "hundreds of young men had pledged to him that they were ready to die and that hundreds of Muslim scientists were with him who would use their knowledge in chemistry, biology and ranging from computers to electronics against the infidels." This statement implies bin Laden is threatening computer attacks against the US. Bin Laden has posted a rambling 11,000 word declaration of war against the US online. This document is known as "The Ladenese Epistle". It calls for the expulsion of the US forces from Saudi Arabia and the overthrow of the current Saudi government. He calls this a jihad or holy war. They are also using websites for propaganda and subverting the minds of Muslim population. These sites allow terrorist organisations to reach ultimate target audience – the worldwide population. Various websites teach surfers the art of computer attack and skills to serve Islam. This has global appeal to young Muslims who can enter the fight without travelling to Afghanistan and risking their lives.

Air Gapped Networks

Nuclear weapons and other sensitive military systems enjoy the most basic form of Internet security. They are "air-gapped," meaning that they are not physically connected to the Internet and are, therefore, inaccessible to outside hackers. The defence and

intelligence computer systems of most countries including India are air-gapped and, thus, isolated from the Internet. It may appear convincing that by air gapping the networks and using superior technology, the risk may be reduced. However, this will not provide adequate security. With the proliferation of technology at an astronomical rate, the threat of cyberterrorism will only increase. Even the air gapped networks are vulnerable from insiders, disgruntled employees and moles planted or recruited by cyberterrorists or their sympathisers to cause the intended damage.

Social Engineering, Dumpster Diving and Trashing. Social engineering is getting information from a person rather than breaking into a system. It is an attempt to have a legitimate user provide the hacker with useful information such as a name and password. Social engineering is a hacker's clever manipulation of humans to gather information needed to access an information system. This method can be employed in person (shoulder surfing), by phone, by dumpster diving or trashing (sorting through discarded trash) or even on-line. 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. Khalid Ibrahim is a member of a Pakistani terrorist group (Harkat-UI-Ansar) and a bin Laden supporter. He is known to use death threats and social engineering to gain information on how to hack the US military networks.[11] He sent certified checks in the mail to potential informants within the US. He was seeking retaliation on the US strikes against Al Qaeda. While it is possible for cyberterrorist to attack without any human interfaces, the human is usually the weakest link in a computer system.[12]

Even Air Gapped Networks are Not entirely Secure. The threat from inside cannot be ignored. Terrorists have options other than a direct hack when it comes to sabotaging manufacturing plants and killing nearby residents. In Russia, hackers used a gas company employee to plant a trojan horse which gave them control of the nation's gas pipelines. In Japan, Aum Shinrykok[13] cult that gassed the Tokyo subway turned out to be a major government and industry software subcontractor. The US State Department recently recalled software from 170 embassies, after realising that

the programmes had been written in the former Soviet Union and could contain dangerous code. Software savvy terrorists could just as easily infiltrate software houses that produce manufacturing process software, and with so much coding done off-shore these days, the potential for problems is even more widespread.

Conclusion

Although the fear of cyberterrorism may be manipulated and exaggerated, we can neither deny nor ignore it. Paradoxically, success in the "war on terror" is likely to make terrorists turn increasingly to unconventional weapons, such as cyberterrorism. And as a new generation of more computer savvy terrorists come, the danger of cyberterrorism is bound to increase.

There is an imperative need to prepare for countering cyberterrorist attacks. It took the tragic events of 11 September 2001 to improve the physical security strategy of many nations. The world should not wait for a cyber tragedy before taking action to improve the security. The attacks are undetectable and victims may not even know that they are being attacked. It is now possible to do what Sun Tzu wrote about 2000 years ago: "conquer an enemy without fighting." Major cyberterror attacks will occur. It is a matter of *when*, not if.

Notes and References

1. Dorothy E Denning, *Networks and Netwars: The Future of Terror, Crime, and Militancy*, p. 281.

2. Barry C, Collin "The Future of Cyber Terrorism: Where the Physical and Virtual Worlds Converge." www.afaen.com/terrorism1.html.

3. Joshua Green. "The myth of Cyberterrorism". www.washingtonmonthly.com/features/2001/0211.green.html.

4. Gabriel Weimann. "Cyberterrorism How Real Is the Threat?", United states Institute of Peace. *Special Report 119*, www.usip.org/pubs/specialreports/sr119.html.

5. Report titled "Cyber-terror: Prospects and Implications" issued by the Center for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School (NPS) in Monterey, California. Downloaded from Eastern Command website of Army intranet.

6. Matt Overholt and Professor Brenner. "Overview of Cyber- Terrorism" http://www.cybercrimes.net/Terrorism/overview.html.

7. Weimann. n. 4.

8. Ibid.

9. Ibid.

10. Col Bradley K Ashley, USAF, "The United States is vulnerable to Cyberterrorism", p. 64.

11. Dorothy E, Denning, "Cyberterrorism." 23 May 2000 Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives www.cs. georaetown.edu/ ~denning/infosec/cyberterror.html

12. S Ramakrishnan "The Security Threat from Cyber Terrorism", *BSF Journal* January 2002, p. 12.

13. Dorothy, n. 1 and n. 11.