Cyber-Terrorism and Cyber Security: A Global Perspective

By: Latha Subrananian, Jianhong Liu, and John Winterdyk[i]

Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb. — National Research Council, *Computers at Risk* (1991).

The term "cyber-terrorism" is, as Peter Gaborsky (2016) pointed out, a somewhat vague term. However, one of the leading experts on the subject defines cyber-terrorism as the "unlawful attacks 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" (Denning, 2000, p. 10). In other words, cyber-terrorism is essentially about the opting of technology to implement terrorist activities. In this article we will provide an overview of how and why cyber-terrorism has become such a major threat to global security and safety.

Cyber Terrorism, Warfare and Threats

Today, cyber space constitutes an arena for a countless number of computing devices that make-up the internet. The presence of autonomous bodies, numerous technological developments posit not merely new advances but also new threats. Cyber space has become the new 'freedom of the press' platform where once only a few had access to such a stage; but today nearly anyone can create a website, post information and engage in virtual communication in real time through the myriad of social media applications. It is estimated that by the end of 2020 that online devices will outnumber human users by a ratio of 6:1. One recent report noted that there are currently around three billion internet users today, compared to a meager 400 million in 2000.

The internet has become a virtual war zone for peacetime hostilities between such countries as Taiwan and China, Israel and Palestine, Pakistan and India, and North Korea and the United States. These virtual interface tensions can involve nation-states, non-state individuals, and groups that either aligned with one side or the other, or groups acting independently. Furthermore, for cyber-terrorists there is no shortage of new tools and new technologies that have allowed them to commit their criminal acts virtually anywhere and from anywhere in the world. As a result, cyber security has become a cornerstone for national and international security policies.

Main forms of cyber threats and the 'tools' of the trade

Although the most common form involves hacking (e.g., Kevin Mitnick in the '70s) and illegally gathering information through social engineering, spreading malwares such as viruses (e.g., Melissa & ILOVEYOU) and worms (e.g., Storm worm in 2007), phishing, spam, pharming, and randsomware.[ii] Other techniques which are being used to commit cyber (terrorist) attack include: data theft, network damage and disruption strategies, the infiltration and destruction of E-governance, E-sources and E-resources, etc.

Why do terrorists opt for cyber space?

There are many reasons for why terrorists opt for cyber space as an option for modern acts of terrorism. Several of these reasons include:

- It is inexpensive. One only needs a technologically equipped person and a personal computers or servers or laptops with internet connectivity or network connectivity.
- The anonymity attached to cyber terrorism is high compared to the traditional terrorist methods. Terrorists use online nicknames —"screen names"—or log on to a website as an unidentified "guest user," making it very difficult for security agencies to identify and locate the identity of the terrorists'.
- It is comparatively easy to attack many targets at one time with less infrastructure and manpower. The sheer number and complexity of potential targets guarantees that terrorists can find weaknesses and vulnerabilities to exploit.
- To commit a cyber (terrorist) attack requires less physical training, psychological investment, risk of injury, etc.
- The time involved in investigating a threat is significant and this time gap allows cyber terrorists to evade detection and apprehension.

- To-date, the investigation and countermeasures for combating cyber threats and terrorisms have been comparatively ineffectual.
- Internationally, there are few international laws or agreements to prevent cyber terrorism or cyber threats.

Prevention of terrorism in cyber space

The ability to prevent cyber terrorism lies with the ability to safely secure cyber space. However, how best can/might cyber space be secured? While we accept cyber terrorism as a form of crime against a nation, group of computers or individuals, it is also understood that any crime involves an offender, a victim or a target space, and a potential Criminal Justice System. In this context application of a few criminological theories would help understanding the prevention strategies. Cohen and Felson in their 1970s Routine Activity Theory on understanding crime problems had elaborately discussed about three major components involved in a crime – a motivated offender, a potential victim and a capable guardian or it is categorized as a handler, a guardian and a manager.

Cyber-terrorists are made not born. They typically enter into cyber-terrorism because they are:

- Attracted towards the terrorist organizations due to their ideologies and support systems, or
- Are trained technological persons and professional hackers who are then hired by terrorist organizations, or
- Represent a new group of individuals who join together to achieve certain goals or a few frustrated individuals try to create damages against the society, or
- Individuals who would like to experiment and show off their capabilities to the world.

Prevention of cyber terrorism through target hardening

For any type of cybercrime, prevention is considered the best means of responding. The terrorists often hide their identity and their whereabouts and they will remain unknown most of the times. This is both true for conventional terrorist activities and for cyber based terrorist incidents. Therefore, one of the primary prevention strategies is the principle of target hardening. For the case of cybercrime prevention, target hardening may be done using various technologies and products (e.g., firewalls, applying cryptology, and intrusion detection) and procedures to protect the information technology assets owned or operated by an individual or organization. It is better to 'harden' the target by minimizing its' vulnerabilities. Given the vulnerabilities of most cyber systems, the low cost of the most attacks, and the ability of attackers to strike from positions of physical safety, a skilled and determined attacker may be more likely to succeed than to become frustrated. Drawing on target hardening concept, it is possible to identify five technological aspects which should be taken into consideration when trying to prevent cyber-terrorism incidents. They include:

1. Strengthening the intelligence gathering applying technology for effectively, evaluating, and acting on intelligence.
2. Securing Supervisory Control and Data Acquisition (SCADA) systems for managing critical physical and telecommunications infrastructures.
3. Upgrading the security of the information assets.
4. Forming emergency response teams in every State of a country.
5. Developing disaster management techniques.

Intelligence is the main source of target hardening. There is a need for having special cyber intelligence teams as we have cyber policing. There is a need for scanning and collecting information regarding the sources and IP addresses of various suspicious organizations, the activities of the existing hacking clubs, professional hackers and their trends in hacking, understanding their modus operandi through which they attack the systems, the latest programming technologies they apply and their association with other countries etc. Unless there is a strong cyber intelligence team, it is impossible to harden the target. Hence, it is essential to secure the critical infrastructure and telecommunication systems through constant monitoring and securing their SCADA systems. As we invest in developing such infrastructures it is also important to invest in security of the systems. Any IT asset is a target for a cyber attacker or cyber terrorist. Hence there is a need for securing the information assets. Hence, every critical infrastructure system should have its own information security policy and planning guidelines.

Similarly, the use of the cloud as a storage space is an invitation to the attackers these days. A cloud is deemed to be unsecured or troublesome for the following reasons:

1. The cloud which is hired from a private agency is operated by someone who is unknown to the customer. It needs a third party provider to maintain the data in the cloud which is one of the most insecure tasks. The customer of a cloud needs to depend on their data security on an unknown source of data regulator. As a result, there is the potential role of cyber-terrorist who may be a part of the third party vendor or the third party vendor may compromise their security without the knowledge of the owner of the data. As such there is no cloud data storage policy or cloud data security.

2. Clouds are vulnerable for cyberattacks as huge amounts of data are being stored in the cloud and no one knows its whereabouts and would be aware of security compromise unless they come to know about the victimization they have undergone. It is easy to steal the passwords of the clouds through phishing and other social engineering techniques.

3. Clouds are additionally prone for insider attacks. An employee can give access to another’s cloud if s/he is disgruntled. Vodafone's breach of 2 million customer records and the Edward Snowden breach at the NSA (i.e., National Security Agency) are wake-up calls the most serious breaches are due to insider threats and privileged user access. The cloud makes this problem 10 times worse since administrative access to the cloud management platform enables access to copy and steal any virtual machine, undetected, as well as potentially destroy the entire cloud environment in very short order.

4. Lack of standardization of clouds is a major problem. There are no uniform norms or legal provisions to regulate the cloud providers, ensure safety, insure the data stored, etc. This makes a cloud provider to have untrained employees. There is a possibility that a cyber-terrorist organization may hire such cloud providing organization or person to get the information from them, steal or damage the data or hack the critical infrastructure in future.

Hence, there is a lot more to think about securing the cloud and protecting the critical infrastructure from the cyber terrorists or cyber attackers. Cyber insurance schemes will be an immediate disaster management scheme to the private and government organizations despite prevention.

The role of a capable guardian in preventing cyber terrorism

There is a need for effective deterrence measures which unfortunately are often lacking in the prevention efforts. In the absence of feasible prevention, deterrence of cyber terrorism may be the next best alternative. Without, at a minimum, a concerted effort at deterrence cyber terrorism will continue to threaten national and international security. Currently, the most feasible way to deter cyber terrorists is to prosecute them under the international law principle of universal jurisdiction (Gable, 2010).

Cyber security has an interesting parallel to terrorism. Both are asymmetric. Ensuring security of data, information, and communication is considerably harder than hacking into a system. The attacker has an inherent advantage in both conventional terrorism and cyberattacks. In the case of state-sponsored attacks, the challenges are of a much higher magnitude (Naraynan, 2016). Defence and protection against cyberattacks is becoming increasingly difficult. This was highlighted at the recent RSA (cyber) Conference 2016 in San Francisco — the RSA is the gold standard of cyber security. The meet acknowledged that “adversaries” (or hackers) were becoming more creative and more sophisticated. At the same time, the industry faced a real shortage of cyber security talent. RSA President Amit Yoran said there are no “silver bullets” in cyber security. Other experts observed that the answer lay in ‘bleeding edge technology’ and ‘big data analytics', a customized approach to specific challenges and a radically new system and data protection architecture that could turn asymmetry on its head.

The aphorism that one needs to be ahead of the curve is relevant to the technology world as a whole. Cyber security is somewhat unique, and rests on the fundamental pillars of mathematics and computer science. The need is to accelerate the pace at which cyber security specialists are produced, to meet the growing threat — one estimate puts the approaching cyber security talent shortage at "almost two million people worldwide". Japan has come out with an action plan for the prevention of cyber-terrorism. United Nations has come out with *Cyber Intelligence Sharing and Protection Act*, 2014. The cyber threat to India cannot be ruled out. The number of attacks on security, military and economic targets is going up. India remains vulnerable to digital intrusions such as cyber espionage, cybercrime, digital disruption and Distributed Denial of Service Coordinated cyberattack could sabotage multiple infrastructure assets, erecting proper defenses is vital. Advances in software are beginning to allow users to browse the Internet anonymously, bouncing actions through 'encrypted relays'. This prevents eavesdropping, determining what sites a particular user is visiting or who the users of a particular site actually are. This, however, could pose other security challenges (Naryanan, 2016).

Conclusion

In recent years, cyber-terrorism has become an increasing global concern. International efforts to combat and/or prevent cyber attackers and/or cyber terrorists is becoming increasingly more challenging as the perpetrators techniques and strategies continually evolve. Therefore, it is ever more important to be forearmed with both offensive cyber operations and strengthened cyber security to effectively combat and prevent the spread of this type of crime. In addition to such initiatives as The Dutch based Hague Security Delta (see https://www.thehaguesecuritydelta.com/), the following points represent some of current prevention strategies:

a) Establish a uniform set of guidelines legislation to prevent cyber terrorism and cyberattacks.

b) Establish and strengthen international cooperation and coordination to more effectively combat the risk of cyberattacks.

c) Increase the level of funding for security measures to government and other agencies.

d) Create uniform cloud computing polices to be derived in with the consultation of various stake holders of all the countries

f) Draft and analyze the risk factors involved in cloud computing and thereby frame counter measures and detection mechanism.

h) Strengthen the education and awareness on information security and digital forensics across the world.

Despite our best intentions and efforts, cyber threats will continue to grow exponentially in the coming years and the resources used to combat will also continue to escalate. It is critical to understand that emerging cyber threats can no longer be ignored, and a continued failure to plan and execute today will cause long-term damage to the security of the country.

References

Denning, D. (2000). "Cyberterrorism." *Global Dialogue* (Autumn). Retrieved from http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc.

Gable, K.A. (2010). Cyber-Apocalypse Now: Securing the Internet against Cyber Terrorism and Using Universal Jurisdiction as a Deterrent", *Vanderbilt Journal of Transnational Law,* 43(1): 100-104.

Grabosky, P. (2016). *Peter Grabosky: Keynotes in criminology and criminal justice: Cybercirme.* New York, NY: OUP.

Narayanan, M.K. (2016, March 19). "The Cyber Threat is Very Real", *The Hindu*, Chennai, India.

[i] **Latha Subrannanian** is Assistant Professor and Secretary, Indian Society of Criminology, Department of Criminology, University of Madras, India.
Jianhong Liu is Professor of Criminology of University of Macau and University Chair Professor at Southwest University of Political Science and Law (SWUPL), China.

[ii] On June 07, 2016, the University of Calgary paid a demanded $20,000 after a ransomeware cyberattack on its computer systems.