CYBER TERRORISM

Vaishnavi Kanchan*

Abstract

In today's world of internet and information technology, the traditional form of terrorism has given way to the more subtle but deadlier form of cyber terrorism. Terrorists are finding cyber terrorism a more convenient way of creating the impact that they desire. And countries are finding themselves ill-equipped to mitigate these threats. In this study we explore the concept of cyber terrorism along with its various definitions. There are several ways and means by which terrorists propagate their agenda. The impact of cyber terrorism can be devastating on countries, resulting in considerable financial loss and political impact. A vulnerability analysis throws up several government and defence networks in India which are critical for the country and could be a target for cyber terrorism. We explore some of the important cyberattack incidents which have impacted countries globally and also incidents which are specific to India. The Government has introduced several initiatives in the cyber security space which include amendments to the IT Act, policy changes and many others. These steps are however not sufficient to mitigate the threats arising out of cyber terrorism. In our concluding remarks we share our recommendations which would help strengthen the fight against this scourge of cyber terrorism.

Keywords: Cyberattack, hacking, critical networks, incidents, government initiatives.

* Student, Government Law College, Mumbai.

Hypothesis

Imagine a terrorist hacking into an air traffic control system of an airport and manipulating its controls, causing planes to collide or crash. Or, another one breaking into a pharmaceutical company's computer systems and changing the formula of its life saving drugs, resulting in thousands of deaths. Or, a terrorist hacking into the computers of a gas utility company, tinkering with the valves and changing pressure in the gas pipes, causing a neighbourhood area to detonate and burn. Or, another one hacking into the country's banking system and the stock exchanges, controlling financial transactions and causing massive disruptions and loss of confidence in the economy. Can these scenarios be a figment of someone's imagination running wild? Or could these be a part of a soon to be released Hollywood movie trailer?

We normally tend to relate the word terrorism with the traditional forms that have existed for quite some time now, and have become mainstay in so many terrorist attacks across the world over the last few years. The internet and information technology have become such an integral part of our lives, that we cannot imagine living without them. Along with its many benefits, it has also brought about several threats. Cyber security has been a point of worry for governments, intelligence agencies and businesses. Cyber crimes, which started off with plain hacking for fun or mischief, have now become financially and politically motivated, and given rise to cyber terrorism.

Technology changes are very rapid, and the face of cyber terrorism has also kept pace with it. Defining cyber terrorism is therefore not easy. Rather than confining it within some strict boundaries, it should be defined in an inclusive and open-ended manner, with provision for the new ways, processes and technologies that are invented regularly to be accommodated into the future definitions.

NATO defines cyber terrorism as "a cyber attack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal". [1]

The FBI in the United States has defined cyber terrorism as a "premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by sub-national groups or clandestine agents". [2]

Another way of defining cyber terrorism is the actions of terrorists which can cause loss of life, worldwide economic chaos and environmental change by hacking into critical infras-

[1] Osman AYTAC, Col Tur Army, Responses to Cyber Terrorism, Centre of Excellence - Defence Against Terrorism – NATO, February 04, 2010, https://www.nato.int/science/2010-02-04-presentations/Osman%20Aytac_COEDAT_cmp.pdf

[2] Thomas Oriti, *Cyberterrorists targeting healthcare systems, critical infrastructure*, ABC NEWS, October 23, 2017, available at http://www.abc.net.au/news/2017-10-23/forget-explosives,-terrorists-are-coming-after-cyber-systems/9076786 (last visited January 01, 2020)

tructure systems.[3] Cyber terrorism is therefore characterized by attacks using computers or internet technology that is motivated by a cause which is political, religious or ideological; with an intention to intimidate governments or a section of the public, and seriously interfere with infrastructure.

I. CYBER TERRORISM: METHODS, MEANS & FORMS

There are three methods by which cyber terrorists attack computer infrastructure.[4]

1. Physical attack: where the computer infrastructure or transmission lines are damaged using conventional methods such as fire and bombs.
2. Syntactic attack: where the logic of the system is tampered with to cause delay or make the system unpredictable. Typically, viruses and Trojans are used in these attacks.
3. Semantic attack: where the information keyed into the system during entering and exiting the system is modified using - coded, without the user's knowledge with the object of inducing errors. These attacks exploit the confidence of the user in the system.

The means and tools used by cyber terrorists to further their agenda include hacking, Trojans, computer viruses and worms. Often email is used as a host by viruses and worms. Email is also used for spreading incorrect and defamatory information and for threats. Denial of service attacks deny authorized people access to a computer or computer network. Terrorists have also started using encryption with high frequency encrypted links, making it extremely difficult to decrypt the information being sent by them. Logic bombs and Chipping are means by which a system is infected and remain dormant till such time conditions arise for activation or until access is desired.

Cyber terrorism supports the traditional form of terrorism such as suicide bombings through the use of computers, internet and information gateways. The most common way of using the internet is by designing websites which promote false propaganda for psychological warfare.

It is difficult to categorize the various forms of cyber terrorism, considering the dynamic nature of technology and the changes and advances which happen frequently. However, we can broadly identify the following forms of cyber terrorism:

a) Violation of privacy
b) Data theft and appropriation of secret information
c) Disruption and demolition of e-governance base
d) Distributed denial of services attack
e) Network disruption and damage

[3] Hardy, Keiran, and George Williams, *What is 'cyberterrorism'? Computer and internet technology in legal definitions of terrorism*, Springer (New York, 2014), https://link.springer.com/chapter/10.1007/978-1-4939-0962-9_1

[4] Cyber Terrorism In India: A Government Nightmare: http://cyberlawsinindia.blogspot.in/2010/01/cyber-terrorism-in-india-government.html (last visited January 01, 2020)

Terrorists have now started preferring cyber attacks compared to traditional methods as they realize its many advantages. Cyber attacks are cheaper than the traditional methods of terrorism. It is difficult to trace the source of action. The terrorists can hide their location as well as their personalities. Using the internet allows the terrorists to escape check points and physical barriers. Terrorists can attack from any location in the world, cover a large number of targets and affect a large number of people.

II. IMPACT OF CYBER TERRORISM

A cyber attack can be launched with the intention of disrupting financial systems and networks or it could be used to support a physical attack with the objective of creating more confusion and delays in response. Cyber terrorism can have a major impact on the economic and social life of the targeted population, with direct and indirect cost implications.

The direct cost implications include the following:

- Impact on sales during the disruption period
- Intermittent access, reduced speed and network delays for business users
- Litigation leading to increased cost of litigation
- Loss of intellectual property – research, design, pricing
- Forensic costs for the recovery and litigation
- Critical communication can be lost during emergency

Indirect cost implications include the following:

- Credibility of financial systems take a severe beating
- Impact on public image globally and tarnished relationships
- Business partner relationships getting strained – both domestic and internationally
- Impact on future business revenue for individual or group of companies
- Loss of trust in the government and the computer industry

III. A VULNERABILITY ANALYSIS

A lot of critical infrastructure is now relying on internet. They include energy, finance, transportation and other essential services. Due to the global nature of information systems, attacks can be launched from anywhere in the world, with very little chances of being detected. The ability of governments to first understand and predict such threats is important, so that necessary measures can be taken to contain them. Access to critical infrastructure is equally important and therefore physical security cannot be isolated from cyber security. Some of the critical networks within the government and defence sectors are discussed below:[5]

[5] Supra note 2

a) Railways: The Indian Railways is one of the busiest in the world. Country Wide Network for Computerized Enhanced Reservation and Ticketing (CONCERT) is one of the largest software projects implemented in India.
b) NICNET: This nationwide communication network is set up by National Informatics Centre (NIC) as the government network.
c) Military: The army has several networks such as Army Radio Engineering Network (AREN) for its field forces, Army Static Switch Communication Network (ASCON) for rearward connectivity from field forces, Army Strategic Information System (ASTROIDS) for exchange of strategic operational information between Army HQ, Command HQ and Corps HQ.
d) ERNET: The Education & Research Network provides network services to Indian academic and research community since 1990 connecting more than 750 organizations.
e) National Stock Exchange (NSE): NSE boasts of over 3000 VSATs covering 425 cities.

IV. INCIDENTS OF CYBER ATTACKS

Terrorist organizations such as the Hezbollah and LTTE used their websites extensively to spread their propaganda. During the terrorist attack at Red Fort by Lashkar-e-Taiba, the militants used a cyber café in North Delhi as a communication link for the operation. There has been an instance of a Swedish hacker who broke into the email accounts of our foreign missions.

Some of the high risk cyber attack incidents are discussed below:

a) In 1998, the LTTE swamped the Sri Lankan embassies with huge number of emails every day for a two week period. The messages read, “We are the Internet Black Tigers and we are doing this to disrupt your communications.” which had the desired effect of causing fear in the embassies. This may have been the first known attack by terrorists against the computer systems of a country.
b) In 1999, hackers protesting against NATO bombing in Kosovo hacked into their computers and flooded them with emails. Public organizations, academic institutions and businesses were flooded with highly politicized emails containing viruses from other European countries. NATO considers the threat of cyber attack as seriously as the risk of a missile strike.
c) Crackers in Romania hacked into the computers controlling the life support system of a research station in Antarctica. The lives of 58 scientists were at risk. However, the hackers were stopped before they could do any real damage.
d) In May 2007, hackers in the Russian Federation subjected Estonia to a massive cyber attack. The attack was in response to the removal of a Russian World War II memorial by Estonia. It was a distributed denial of service attack, wherein specific

sites were flooded with traffic, forcing them to go offline. The Estonian government networks and the network of two major Estonian banks were forced to go offline by the attacks. Moreover, the Prime Minister's political party website was hacked and a fake letter was posted with his apology for removing the memorial statue.

e) In 2017 there were several cyber attacks which shook the world. The WannaCry ransom-ware hit public utilities and large corporations, particularly the National Health Service (NHS) hospitals and facilities in the UK. This ransom-ware affected the emergency rooms at the hospitals, delayed vital medical procedures and caused chaos for British patients.[6]

f) Another malware which affected people globally in 2017 was Petya/NotPetya. It affected the US pharma company Merck, the Danish shipping company Maersk and the Russian oil giant Rosneft. The Ukrainian infrastructure was hit the hardest, disrupting utilities such as power companies, airports, public transit and the country's central bank. In the Asia Pacific region, India was the most affected and the seventh most affected globally.

g) In another incident in 2017, hackers penetrated Equifax, the largest credit bureau in the world and stole personal data of 145 million people. This is considered to be one of the worst hacking incidents ever, because of the sensitivity of the information stolen.

h) In the most recent case on April 7, 2018, the Iranian IT Ministry has reported that computer systems in Iran, along with several other countries, including India were hacked to display an image of the US flag on computer screens. The image was displayed along with a warning "Don't mess with our elections". The attack has affected 200,000 router [7]switches globally, including 35,000 switches in Iran. The attack has hit internet service providers and cut off web access for their subscribers. The hackers exploited vulnerability in certain Cisco routers, for which Cisco had sent a warning along with a security patch. Those who failed to apply the patch on time have been affected.

V. CYBER ATTACKS IN THE INDIAN CONTEXT

India is vulnerable to cyber terrorism and an attack can bring the country to a standstill with long term impact on business and investment. During some of the incidents related to blasts at Ahmadabad and Delhi, criminals were found to have hacked into the wifi system of individuals to send terror emails. When the Mumbai Police arrested around 20 suspected members from the Indian Mujahideen (IM) in October 2008, they found 4 IT savvy members amongst them. They were responsible for

[6] Josh Fruhlinger, *What is a cyber attack? Recent examples show disturbing trends*, CSOONLINE.COM, March 7, 2018, https://www.csoonline.com/article/3237324/cyber-attacks-espionage/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html

[7] Ibid note 6

sending emails in the name of IM before and after the Ahmadabad blasts and before the Delhi blasts by hacking into wifi networks in Mumbai and Navi Mumbai. Such incidents demonstrate the kind of risks involved in cyber attacks.

Cyber terrorism between two countries can transform into cyber attacks and ultimately all-out cyber war. The situation between India and Pakistan is in a similar condition. Pakistani hackers have targeted in the past the Gujarat Government, Ministry of External Affairs, Indira Gandhi Centre for Atomic Research, India Online Bazaar, Indian National IT Promotion, India Today, Nuclear Science Centre and Telecom companies.

In another incident, a Swedish security professional called Dan Egested hacked into email accounts of 100 senior Indian government officials, including embassy officials and DRDO officials and posted the passwords on the internet. Access to confidential information could have had serious consequences on national security.

In another incident, the website of a major bank was hacked and infested with malware. Any individual who visited the home page of the bank automatically downloaded around 22 Trojans. Some of the Trojans had the ability of "key loggers", which could compromise the security of all the bank's customers.

In another incident, a chartered accountant from Ahmadabad, in a well-publicized TV program demonstrated how he could put through a call in the name of the home minister to another minister. This is an example of SMS/Phone spoofing through the websites.

In another incident, the website of the National Police Academy was hacked and a phishing site published in its place.

In 2016, India's IRCTC website came in the news when reports claimed that the site had been hacked. Data of around 10 million clients was feared to have been stolen from the e-ticketing portal. While IRCTC denied the hack and issued an official statement, a cyber security start-up company showed how exactly the data leak can happen easily on the IRCTC website.[8]

In 2017, India saw a number of cyber attacks. The WannaCry and Petya ransom-wares which affected computers globally were also responsible for creating havoc in India.[9]

In an incident in 2017, state run telco BSNL's broadband network in Karnataka was hit by malware, affecting around 60,000 modems. These modems could not connect to the internet. Users were forced to change their user names and passwords in order to rectify the problem.

[8] Komal Mohan, *5 recent cyberattacks you might have missed*, GADGETSNOW.COM, June 8, 2016, https://www.gadgetsnow.com/slideshows/5-recent-cyberattacks-you-might-have-missed/photolist/52634364.cms

[9] Samden Sherpa, *Cyber attacks that affected India in 2017*, GIZBOT.COM, December 22, 2017, https://www.gizbot.com/internet/features/cyber-attacks-that-affected-india-in-2017-046533.html

In May 2017, Zomato the Indian restaurant search service reported that their company database was breached and personal details of close to 8 million users stolen. The leaked information was also listed for sale. Zomato contacted the hacker and struck a deal, after which the data was brought down.

Reliance Jio was also a victim of data breach last year. A website called magicapk.com went live after the data breach attack and published personal details of Jio users on the site. The website was taken down after it went viral.

The Indian Computer Emergency Response Team (CERT-In) issued an advisory in July 2017 against the Mirai Botnet malware which affected home router users and IoT devices across the globe. It is a Distributed Denial of Service (DDOS) malware. This malware hit 2.5 million IoT users globally, though its exact impact in India is not known.

On Jan 1, 2017, some unknown hackers hacked into the NSG website and partially defaced it and posted abusive language. From 2014 onwards till Nov 2017, out of 8000 websites hosted on NICNET, 248 government websites were defaced.[10]

Between Nov 2016 and June 2017, 50 cyber attacks were reported on 19 financial organizations. In 2016, there were over 50,000 cyber security incidents which included 757 cases of phishing, 416 cases of network scanning, 13,371 cases of virus and malicious code, 31,664 cases of website defacements, 1483 cases of website intrusion and malware propagation.[11]

VI. INITIATIVES TO COUNTER CYBER TERRORISM

The Government of India has taken some initiatives to counter the threat of cyber terrorism. Some of these initiatives are discussed below:

Indian Computer Emergency Response Team (CERT-In): This is the functional organization of the Department of Information Technology and has the objective of securing the Indian cyber space. Its proactive services include advisories, security alerts, vulnerability notes and security guidelines. The reactive services include minimizing damage of security incidents. 25 cyber security exercises have been conducted in organizations in finance, defence, power, telecom, transport, energy, space, IT/ITeS sectors for checking preparedness. 22 training programs covering 610 participants were conducted last year for network/system administrators. [12]

Cyber Crisis Management Plan has been formulated for countering cyber terrorism in all Centre and State ministries and critical sectors.

National Cyber Security Assurance Framework: It is established by CERT-In for the protection of critical information

[10] ET Bureau, *Cyber threat to government websites: A look at the data*, April 7, 2018, https://economictimes.indiatimes.com/tech/internet/cyber-threat-to-government-websites-a-look-at-the-data/articleshow/63659529.cms

[11] Ibid note 10

[12] Supra note 9

infrastructure. Security auditors have been empanelled for auditing, undertaking vulnerability assessment and penetration testing of the computer systems and networks of the government and critical organizations. 67 security auditing organizations have been roped in for these checks.[13]

National Cyber Coordination Centre (NCCC) generates situational awareness of existing and potential cyber security threats. Phase – 1 of the NCCC has been made operational.

Collaboration with Vendors: CERT actively collaborates with IT product and security vendors such as Microsoft, Cisco, RedHat, McAfee, Symantec, etc. for security assurance.

International Collaboration: CERT also actively collaborates with international security organizations and CERTs of other countries for information exchange on latest cyber security threats and best international practices in this area.

Indo–US Joint Working Group: This Indo-US group on counter terrorism was formed in Jan 2000 with a commitment to improve bilateral cooperation as part of the global effort against terrorism.

Internet Security Centre: This $20 million centre was established in New Delhi by the Ministry of Information Technology in 2003 and addresses computer security incidents, publishes alerts and promotes training and information. The Software Technology Parks of India (STPI) has a stake in the centre.

Centre for Development of Advanced Computing (C-DAC) and Defence Research and Development Organization (DRDO) are organizations associated with this centre. Membership is open to private and public sector organizations. A lot of work in the area of cyber security has happened at this centre, including work by the Indian Navy in collaboration with IIT Kanpur and several private organizations in the area of security solutions.

Defence Information Warfare Agency (DIWA): This agency has been established by the armed forces and manages all aspects of Information Warfare such as psychological operations, cyber war and electromagnetic and sound waves. It is the nodal agency which makes policies for the armed forces with regard to enemy countermeasures and propaganda.

Resource Centre for Cyber Forensics (RCCF): The RCCF was set up at the CDAC centre at Thiruvananthapuram. It will develop cyber forensics toolkit, carry out R&D work in cyber forensics area and provide technical training to agencies. Several tools for cyber forensics such as disk forensics, network forensics and device forensics have been developed by RCCF.

Information Technology Act, 2000: The 2009 amendment of the IT Act has recognized cyber terrorism and has made provision for the same under Section 66-F. It prescribes a punishment for cyber terrorism which can extend to life imprisonment. The IT Act has also authorized

[13] Supra note 9

CERT-In as the nodal agency with regard to Critical Information Infrastructure for coordinating all actions related to information security practices, guidelines, incident prevention, response and report.

VII. CONCLUSION

India has recognized the threat that cyber terrorism holds out and has taken several initiatives in the area of cyber security to mitigate these threats. However, a lot more needs to be done by the Government and businesses to address areas such as risk assessment, security design, security management, reassessment of information systems and tools and their implementation. Some of the measures that we could take are discussed below:

- Risk Management: Effective risk management does not involve just the deployment of the latest security product. Every defensive move will be countered by an attacker with even stronger measures. A more complete approach would be proactive and process oriented, involving – risk assessment, development of counter measure plans, execution of counter measures and testing the measures implemented.
- Regular Threat Analysis: A regular threat analysis is required to identify physical, electronic and procedural shortcomings. It will help to identify resources that need extra protection and monitoring for safety.
- Vulnerability Audit: We need to identify assets and critical national resources which use cyber space for transactions, whose loss can cause serious damage to our country.
- Deny the Medium: Terrorists use cyber space to communicate and coordinate their activities. Denying them this medium can help to control this issue. However, such steps can violate individual privacy and affect knowledge based industries. There is a need to balance the two.
- Cooperation between Intelligence and Cyber Policing Agencies: Such cooperation between agencies will bring together hard intelligence and cyber monitoring mechanisms, which would help to track criminals and terrorists.
- Create a culture of cyber security awareness by educating the masses on cyber security, both on physical hardware and computer software.
- Initiatives to mitigate bots, botnets and distributed denial of service attacks should be taken up by the government at the national level along with ISPs.
- Risk Mitigation Plan / Disaster Recovery Plan should be in place and should be tested at regular period of time.
- While the IT Act has recognized cyber terrorism, it still lacks innovativeness and futuristic vision. There is a need to put a strong Cyber Law in place for the purpose of tackling cyber terrorism.
- Cyber Forensic Capability needs to be strengthened further and IT laws should support state sponsored cyber forensics for the purpose of tracking down terrorists.

- Crytographic Analysis capability should be further strengthened so as to crack encrypted traffic and passwords used by terrorists.
- Best Practices, Cyber Audits & Intern-ational Cooperation: The Gover-nment and businesses must build procedures which are commensurate with interna-tional best practices. Certified com-panies need to do regular audits of web-sites and services. International coope-ration should be encouraged in sharing of information, forensic software, crypto analysis, and building a handshake on IT laws that deal with handling of terrorists.
- Cooperation between Government and Private Industry for the purpose of cyber security should be further strengthened.

The time has come when we should prioritize cyber security in our counter terrorism strategy. While some baby steps have been taken in this direction and several new initia-tives are underway, there is a need to for a lot to be done in this area. Implementing a strong law on cyber terrorism and strengthening cyber security through the recommendations given above will hopefully put India on the path to a strong and secure cyber space.