Research Paper Political Science

Spectre of Cyberterrorism: A Potential Threat to India's National Security

Dr. Amar Singh | Researcher, Centre for South Asian Studies, School of International Relations, JNU, New Delhi.

ABSTRACT

Cyber security has quickly evolved from a technical discipline to a strategic concept. Globalization and the Internet have given individuals, organizations, and nations incredible new power, based on constantly developing networking technology. For everyone – students, soldiers, spies, propagandists, hackers, and terrorists – information gathering, communications, fundraising, and public relations have been digitized and revolutionized. As a consequence ,the use and abuse of computers, databases, and the networks that connect them to achieve political and military objectives now have a cyber dimension, the size and impact of which are difficult to predict, and difficult to retaliate as well. A cyber attack is not an end in itself, but a powerful means to a wide variety of ends, from propaganda to espionage, from denial of service to the destruction of critical infrastructure. The nature of national security threat has not changed, but the Internet has provided a new delivery mechanism that can increase the speed, scale, and power of an attack. However, the question arises here is that, can a cyber attack pose a serious threat to national security?

KEYWORDS

Introduction:

In 1948, Hans Morgenthau wrote that national security depends on the integrity of a nation's borders and its institutions. However in 2016, everything from elections to electricity, are computerized and connected to the Internet, the terrestrial distance between adversaries can be irrelevant because everyone is a next-door neighbor in cyberspace. The next wave of national security threats, therefore, might originate from cyberspace. It is a complex and multidimensional problems against which no degree of technical superiority is likely to suffice. The drumbeats of cyberwarfare has in place of have been sounding for years. Network intrusions are widely viewed as one of the most serious potential national security, public safety and economic challenges. Technology, in this case, becomes a double-edge sword. Cyber attacks can not only quickly harm data and computing networks, but also damage computer-controlled critical infrastructure, such as electric power, telecommunications, water supply, air traffic, and first-responder communications. Given the complex interconnections between infrastructure components, an attack on a single sector could lead to cascading failures, with potentially devastating consequences. This shows that the very technology that empower us to lead and create also empower individual criminal hackers, organized criminal groups, terrorist networks and other advanced nations to disrupt the critical infrastructure that is vital to our economy, commerce, public safety, and military security. In cyber world last decade has seen mostly exploitation by adversaries, or the theft of money and intellectual property. Next come distributed denial of service attacks when hackers overwhelm networks and disrupt operations organizations, future can be devastating, as an adversary seeking to reach out and harm India has now one other option: destructive cyber-attacks, all of that is within the realm of the possible."[2]

Cyberthreats

Cyber attacks are defined as "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[3] Cyber threats can be disaggregated, based on the perpetrators and their motives, into four baskets:

- ***Cyber espionage:*** Penetration of adversary computers and networks to obtain information for intelligence purposes;
- ***Cyber warfare:*** Actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.[4]
- ***Cyberterrorism:*** Non-state actors (terrorists or syndicated criminal networks)whose intent is disruptive and who may be subject to the jurisdiction of one or more sovereign states.
- ***Cyber crime:*** Insider fraud and external organizations that are infiltrating ranks and using them to infiltrate data from organization.[5] Cyber attackers use numerous vulnerabilities in cyberspace to commit these acts. They exploit the weaknesses in software and hardware design through the use of malware. DOSs (Denial of services) attacks are used to overwhelm the targeted websites. Hacking is a common way of piercing the defences of protected computer systems and interfering with their functioning. Identity theft is also common. The scope and nature of threats and vulnerabilities is multiplying with every passing day.[6]

Definition of Cyber Terrorism:

Information technology (IT) has exposed the user to a huge data bank of information regarding everything and anything. However, it has also added a new dimension to terrorism. Recent reports suggest that the terrorist is also getting equipped to utilize cyber space to carryout terrorist attacks. The possibility of such attacks in future cannot be denied. Terrorism related to cyber is popularly known as 'cyber terrorism'. "Cyber terrorism is the convergence of terrorism and cyber space. It is generally understood to mean unlawful attacks and threats of attacks against computers, networks, and 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 asset 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 upon their impact.[7]

Cyber terrorism encompasses attacks against life and electronic infrastructure which are directed against national security establishments and critical infrastructure. The aim of the attacks is to cause a state of terror and panic in the general public.[8] Unfortunately, cyberterrorism remains a viable option

for any individual or group wanting to use it to further their goals. While bombing physical targets may attract unwanted attention and raise the risk of failure, cyberterrorist attacks can be orchestrated more accurately and easily, and due to the remote location of the preliminary step, the perpetrators are less detectable.[9]

Methods of Attacks:
The most popular weapon in cyber terrorism is the use of computer viruses and worms. That is why in some cases of cyber terrorism is also called 'computer terrorism'. The attacks or methods on the computer infrastructure can be classified into three different categories.

- ***Physical Attack:*** The computer infrastructure is damaged by using conventional methods like bombs, fire etc.
- ***Syntactic Attack:*** The computer infrastructure is damaged by modifying the logic of the system in order to introduce delay or make the system unpredictable. Computer viruses and Trojans are used in this type of attack.
- ***Semantic Attack:*** This is more treacherous as it exploits the confidence of the user in the system. During the attack the information keyed in the system during entering and exiting the system is modified without the users knowledge in order to induce errors, [10]

Terrorists can also use the Internet for organisational purposes rather than to commit acts of terror like; propaganda, information gathering, preparation of real-world attacks, publication of training material, communication, and terrorist financing. This means that organisations or governments which depend on the operation of computers and computer networks can be easily attacked.[11]

India's Cyber Vulnerabilities:
In the circle of national security policy making, criminal hacking, terrorist networks, nation-states conducting espionage, threats to critical infrastructures or services are the most important security concerns. Among the most seriously assessed cyber attacks on Indian interests are the espionage campaign by GhostNet, Chinese espionage activities [against DRDO in March 2012 and Indian Navy's Eastern Command in June 2012] and attack on Indira Gandhi International Airport network.[12] However global concerns about India's net security practices rose after 25 June 2015, when hackers broke into the National Informatics Centre (NIC), which runs e-mails of all central government officials as well as websites of various ministries and scheme and accessed information on its root directory that hosts the sensitive data. They issued several fake digital certificates which went undetected for days. A survey by a government agency shows over 780 attacks that damaged sensitive computers across 88 cities and over 350 hacking attempts on sensitive computer systems last year.[13] It has always been difficult to trace the origin of a cyber threat and cyber crime. According to a report, India ranks second in social media scams and third in Asia for ransomware attacks and sixth in being the most bot-infected country.[14]

Challenges to India's National Security:
The convergence of the physical and virtual worlds has resulted in the creation of a "new threat" called cyber terrorism. The concern with the threat of cyber terrorism stems from a combination of fear and ignorance. The failure to distinguish between hacktivism and cyber terrorism has also contributed to the fear and hype about the threat of cyber terrorism. However, the number of potential targets and the lack of proper and adequate safeguards have also made addressing the threat a daunting task.[15]

India's cyberspace is linked to that of the rest of the world. Mounting defences against attacks occuring at lightning speed and distinguishing between malicious activity originating from criminals, nation-states, and terrorists in real-time is difficult. Systems supporting a country's critical defence and intelligence community must be secure, reliable and resilient enough to withstand attacks, regardless of their place of origin. By the turn of the 21st century, virtually all known terrorist groups had secured a presence on the internet. There is overwhelming evidence of terrorist groups utilising the internet to engage in psychological warfare, propaganda, data mining, fund raising, recruiting, networking, information sharing, and planning and coordination. Terrorists nowadays are highly sophisticated in their use of weapons, communications and planning techniques. They operate in a highly decentralised manner, which makes them more difficult to locate and track than a small cell of a terrorist group at any given time. These groups are using the internet to collect open-source information to be used for the preparation and execution of their operations.[16]

Post liberalization, Information Technology (IT), electricity and telecom sector has witnessed large investments by private sector in India. However, inadequate focus to disaster preparedness and recovery in regulatory frameworks is a cause of concern. No single operator controls the IT, Telecom or Power sectors and, therefore, responsibility to prepare for, and recover from, disasters is diffused. Taking this into account government has to come up with a comprehensive disaster preparedness and recovery strategy. As India is marching towards e-governance and e-commerce, vulnerability of this infrastructure to natural and manmade disaster and consequent cascading effect on our national security remains unarticulated.[17]

Response of government:
In 1999 Indian government created a new ministry of information technology (MIT) by merging the department of electronics (DOE), national informatics centre (NIC) and electronics and software export promotion council. The Information Technology Act of 2000 contained no provision on cyber terrorism. However, this lack of cyber security strategy was rectified when the Information Technology Amendment Act of 2008 was promulgated as it contains a provision on cyber terrorism. Section 66F defines and penalises cyber terrorism. In order to qualify as a cyber terrorist act, the act must be committed with the intention to threaten the unity, integrity, security or sovereignty of India by way of interfering with authorised access to a computer resource, obtaining unauthorised access to a computer resource or damaging a computer network. The acts are punishable if they cause death or injuries to persons or cause damage or destruction to property, disrupt essential supplies or services or affect critical information infrastructure. The penalties range from three years' imprisonment to life imprisonment and a fine depending on the seriousness of the crime.[18]

However 2004, the government set up the Indian Computer emergency response Team (CerT-In) in line with its evolving cyber security measures.[19] CERT-In functioning under DIT is India's response to cyberthreats. It has been established to respond to the cyber security incidents and take steps to prevent recurrence of the same. "The purpose of the CERT-In is, to become the nation's most trusted referral agency of the Indian Community for responding to computer security incidents as and when they occur. Furthermore it will also assist members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents."[20]

Furthermore Indian government is creating a centralized mechanism to coordinate and analyze information gathered from internet accounts throughout the country. It will be called the National Cyber Coordination Centre [NCCC]. The NCCC will facilitate real-time assessment of cyber security threats in the country and generate actionable reports/alerts for proactive actions[21] by coordinating intelligence and cyber response agencies such as the Research and Analysis Wing (RAW), National Technical Research Organization (NTRO), Defense Research and Development Organization (DRDO), Department of Telecommunications, CERT-In, Intelligence Bureau (IB) and the different Indian military services to ensure a more robust defence of critical Indian computer systems.[22]

Strategic Objectives for Cyber Defence

Forming a viable national strategy for cyber defence, any nation would be guided by its ability to meet its technical, economic and security needs. An achievable strategic objective for a developing country like India in the not too distant future (5-10 years) could be:

- Prevent cyber attacks against information systems and IT based/dependent infrastructures.
- Reduce the overall national vulnerability to cyber attacks.
- Minimise damage and reduce recovery/resuscitation time from cyber attacks that do occur.[23]

Recommendations:

- To designate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities
- Strengthened security models should be adopted to protect critical sectors of infrastructure and security establishments.
- Need of qualified manpower to implement the counter measures, specific training must be provided in order to assist users in IT security. [24]
- rapid identification and information exchange methods should be adopted to counter any malicious cyberspace activities .
- Establish a public – private architecture for responding to national- level cyber incidents.
- Cyber security audits should be made compulsory for networked organizations. The standards should be enforced through a combination of regulation and incentives.
- The government should launch a National Mission in Cyber Forensics to facilitate prosecution of cyber criminals and cyber terrorists.

Conclusion:

Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation- states and non-state actors. The day is not far when terrorists themselves will cause large-scale cyber incidents as they have already graduated from defacing websites to causing real damage to their "enemies," especially their critical infrastructure. This will change the entire landscape of terrorism. A common vision is required to ensure cyber security and prevent cyber crimes. The time has come to prioritize cyber security in India's counter terrorism strategy.

Endnotes:

1 Sandra I. Erwin et all. (2012), "Top Five Threats to National Security in the Coming Decade", retrieved from URL:http://www.nationaldefensemagazine.org/archive/2012/november/pages/topfivethreatstonationalsecurityinthecomingdecade.aspx

2 Data Security Council of India (2015), "Cyber Attacks", retrieved from URL https://www.dsci.in/taxonomypage/242

3 Ibid.

4 Devendra Parulekar (2014), "Cyberspace: A focus on India", retrieved from URL: http://www.ey.com/Publication/vwLUAssets/EY-CFO-need-to-know-cyber-security-a_focus-on-india/$FILE/EY-CFO-need-to-know-cybersecurity-a-focus-on-india.pdf …

5 "Cybersecurity–An Overview"(2012), in "India's Cyber Security Challenge", IDSA Task Force Report, New Delhi

6 Col. S S Raghav (2010), "Cyber Security In India's Counter Terrorism Strategy", retrieved from URL: http://ids.nic.in/art_by_offids/Cyber%20security%20in%20india%20by%20Col%20SS%20Raghav.pdf

7 Ibid.

8 Tara Mythri Raghavan (2003), "In Fear of Cyberterrorism: An Analysis of the Congressional Response", Illinois College of Law, USA.

9 Raghav(2010), op. cit., no6

10 F Cassim (2012), "Addressing the Spectre of Cyber Terrorism: A Comparative Perspective", retrieved from URL: http://www.saflii.org/za/journals/PER/2012/27.html

11 Dr Omair Anas (2015), "In search of India's Cyber Security Doctrine", ICWA Policy Brief, New Delhi.

12 "Centre to Shield India from Cyber Attacks Proposed" (2014), The Hindustan Times, 17 August, New Delhi.

13 Anas (2015),op. cit., no11

14 Cassim (2012), op. cit., no10

15 S R R Aiyengar(2010), "National Strategy for Cyberspace Security", Manekshaw Paper no. 23, Centre for Land Warfare Studies, New Delhi

16 M M Chaturvedi and MP Gupta and Jaijit Bhattacharya (2015), "Cyber Security Infrastructure in India: A Study", Department of Management Studies, Indian Institute of Technology Delhi, New Delhi.

17 Cassim (2012), op. cit., no10

18 Anas (2015),op. cit., no11

19 M M Chaturvedi and MP Gupta and Jaijit Bhattacharya (2015), op. cit., no16

20 Zachary Keck(2013), "India Sets Up Domestic PRISM-Like Cyber Surveillance?", the diplomat, June 14, http://thediplomat.com/2013/06/india-sets-up-domestic-prism-like-cyber-surveillance/

21 "Centre to Shield India from Cyber Attacks Proposed"(2014), The Hindustan Times, 17 August, New Delhi.

22 S R R Aiyengar (2010), op. cit., no15

23 Anoop Kumar Verma and Aman Kumar Sharma (2014), "Cyber Security Issues and Recommendations", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4: 4, April.