International Journal of Advanced Research in Engineering Technology & Science ISSN: 2349-2819
Email: editor@ijarets.org Volume-6, Issue-11 November- 2019 www.ijarets.org

CONSCIOUSNESS OF THE CYBER-SECURITY IN INDIA

Vipin Kumar Thakur
Research Scholar
Shri Venkateshwara University
Gajraula

Dr.Manoj Kumar
Associate Professor
Shri Venkateshwara University
Gajraula

ABSTRACT
The Government of India has identified Militarisation of Space and Cyber Security as one among the five medium term threats/challenges faced by our country. The spectre of nuclear proliferation and cyber terrorism and their connection with international terrorism also represent problems for Indian national security for which solutions must necessarily rely on international cooperation. "The apparent stability of the nuclear balance and the quest for seeking new areas for military advantage may prompt some states to move towards weaponisation of space. India, with its yet limited space capability, will face a major challenge in protecting its space assets in case of a conflict. Similarly, cyber space will be a greater challenge going forward— both for security and economy"
Key words: Cyber Security, international terrorism

INTRODUCTION
India on its growth path is vulnerable. Located in an unstable region where the larger neighbours possess this capacity, it is logical to assume that the country is under serious threat and constant attack. The impact on national security is thus serious and such that all institutions and organs of the state must jointly work to counter this challenge. The Government of India has recently taken several steps to ensure greater focus on these issues within the country. It has recently notified the National Cyber Security Policy 2013 with the goal of addressing the cyber security domain comprehensively from a national perspective. The main goal of the policy is to make the cyberspace secure and resilient for citizens, businesses, and the government. The policy envisages the establishment of national and sectoral mechanisms to ensure cyber security through the creation of a National Critical Information Infrastructure Protection Centre (NCIIPC). Computer Emergency Response Team (CERT-In) shall act as the nodal agency for coordination of all cyber security and crisis management efforts. It will also act as the nodal organisation for coordination and operationalization of sectoral CERTs in specific domains in the country.

Though efforts are being made to create an effective policy framework to deal with cyber security in the country, there are areas where significant challenges lie. E-governance is a specific case in point. The country has put in place a separate core ICT infrastructure for e-governance consisting of statewide area networks (SWANs) and state data centres (SDCs) in each state and union territory. Common Service Centres (CSCs), run by private village level entrepreneurs (VLEs), act as the front end for delivery of these services in rural areas. Currently, over 100,000 CSCs are operational across the country. Recently, mobile governance has been implemented to bring all government services on the mobile platform. The National e-Governance Plan is the flagship programme in e-governance consisting of 31 Mission Mode Projects (MMPs) spanning across a large number of government ministries and departments both at the national and state levels. During the last seven years of its implementation, NeGP has achieved considerable success with 23 out of the 31 projects delivering services electronically to the citizens and businesses.

Though National e-Governance Plan (NeGP) has been a success, ensuring cyber security remains a big challenge as it involves protecting critical ICT infrastructure such as SWANs, SDCs and the applications of various departments running on them. Though scheme specific guidelines have been issued and several states have made significant efforts to protect their cyber assets, there is a need

for a comprehensive policy on cyber security in e-governance and ensuring uniformity in its implementation across the country. Application level security is another important domain where greater effort is required.

Building a national strategy for cyber security is the first step in establishing a national cyber security program. A national policy framework should explain the importance of cyber security; help stakeholders understand their role, and set goals and priorities. The national strategy should integrate security fundamentals (such as raising awareness) and emphasize cooperative relationships among national stakeholders. The national strategy can also serve as a backdrop for the creation of laws that relate to areas such as computer crime, the protection of intellectual property, and privacy. The goals that a nation identifies and promotes through its strategy align the program to a consistent vision and establish a clear direction for the efforts of the program. The strategy should include sufficient detail to allow stakeholders—including the National CSIRT—to understand the stated goals and evaluate their progress toward achieving them. Finally, the national strategy should reconcile the need for security with the rights of citizens, as well as national values and norms.

The National CSIRT should be deliberately aligned with national cyber security strategic goals to ensure that its work contributes to achieving them. While establishing a national strategy is the first step, doing so may not always be feasible. Getting a large number of stakeholders to agree on a strategy can be difficult. Alternatively, national leaders may judge that the need to establish an incident management capability is more pressing than creating a fully integrated strategy. In these cases, creating an effective strategy may occur concomitantly with building incident management capability. Regardless, the National CSIRT sponsor or proponent should work with the government to consider national needs and priorities throughout the process of building a National CSIRT.

India's approach to cyber security has so far been ad hoc and piecemeal. A number of organisations have been created but their precise roles have not been defined nor has synergy been created among them. As it transcends a vast domain, this falls within the charter of the NSCS. However, there appears to be no institutional structure for implementation of policies. Neither the private sector nor government has been able to build information systems that can be described as reasonably robust. There has not been enough thinking on the implications of cyber warfare.

India and China's cyber security preparedness is a striking study in contrast. India is a reputed information technology-enabled nation while China struggles with its language handicap. India, with a massive 243 million internet users, has digitized its governance, economy and daily life on an industrial scale without paying adequate attention to securitize the digitization plan. In the digital era, national security is inextricably linked with cyber security, but despite being the single biggest supplier of cyber workforce across the world India failed to secure its bandwidth and falters to detect the simplest of cyber crimes, which often leads to devastating consequences.

KEY STAKEHOLDERS OF NATIONAL CYBER SECURITY

Governments have a multitude of roles and responsibilities to strengthen national cyber security. Their primary role is to define national strategy and provide the policy framework. The policy framework of any government describes the architecture by which national efforts are built and operated. Following that, the government has a responsibility to participate with all stakeholders in efforts to identify, analyze, and mitigate risk. The government also has a key role to play in the arena of international relations and cyber security, particularly in the creation of treaties relating to cyber security and the harmonization of national laws relating to cybercrime.

Executive Branch of the Government

In most nations, the executive branch enforces laws and ensures security. It also may include the military. The executive branch is often the sponsor of the national cyber security program. They

ensure that the cyber security program remains viable and has appropriate resources (for example, is authorized, staffed, funded, and so on).

Legislative Branch of the Government

The legislative branch provides effective laws that promote cyber security. Whether through appropriations of resources or funding, legislation that mandates execution of national strategy, privacy or tort laws, or laws that establish criminal behaviors, the legislature must ensure that national cyber security program has necessary support.

The Judiciary

The nation's judiciary and legal institutions provide clarity and consistency in areas of law that can affect cyber security. Privacy law is an example of one of these areas. By working with their global counterparts, the legal community can limit the ability of criminals and other malicious actors to take advantage of differences in legal jurisdictions.

Law Enforcement

Law enforcement ensures that legislation related to cyber security is enforced. Additionally, law enforcement can serve as an important source of intelligence about malicious activity, exploited vulnerabilities, and methods of attack. Sharing this information allows critical infrastructure owners and operators to learn from others' experiences and improve security practices and management. Law enforcement can also enhance cyber security by cooperating with counterparts in other nations on the pursuit and apprehension of international criminal actors.

CYBER SECURITY ACTORS IN INDIA

The draft cyber security policy document put out by the Department of Information Technology (DIT) for public discussion is an important step but it is essentially a departmental effort, not taking a whole- of-government approach. DIT does not have jurisdiction over departments.

The document lists a number of major stakeholders, including:

- National Information Board (NIB);
- National Crisis Management Committee (NCMC);
- National Security Council Secretariat (NSCS);
- Ministry of Home Affairs (MHA);
- Ministry of Defence (MoD);
- Department of Information Technology (DIT);
- Department of Telecommunications (DoT);
- National Cyber Response Centre (NCRC);
- CERT-In; (Computer Emergency Response Team – India)
- National Information Infrastructure Protection Centre (NIIPC); (11) National Disaster Management Authority (NDMA);
- Standardisation, Testing and Quality Certification (STQC) Directorate;

INDIA'S CYBER PREPAREDNESS

To guarantee and retain information superiority, appropriate defensive measures and countermeasures are a must.While the debate on the exact definition of critical information infrastructure (CII) rallies on, the IT (Amendment) Bill 2008 attributes the designation of a national nodal agency for the protection of CII and the Indian Computer Emergency Response Team (CERT-In) to undertake incidence response under the Sections 70A and 70B, respectively.11 MoD also mandates Defence agency Information Assurance and Research Agency (DIARA) as the nodal cyber security for the Tri-Services.12 However, substantive resolution is needed on the role imparted to the National Informatics Centre (NIC), the IT infrastructure services organisation managing a majority of the government websites. A government-wide information security and regulatory compliance policy, dealing with issues like electronic document classification,

compartmentalisation and centralised security clearance, is also the need the hour.

Any attempt to arrive at a possible solution to the aforementioned issues from a geopolitical, strategic affairs and policy making perspective will need a holistic approach taking into account the technical, legal and international complexities. India's National Security Advisor proposed the ratification of a global cyber-security regime or a cyber-arms control treaty.13 Similar endeavours of international regulation in domains like chemical, nuclear and space warfare have been impactful. The primary stakeholders are even receptive to the idea of re-engineering the underlying communication protocols of the Internet to reach a level of moderation. While most nations, including those engaged in questionable activities over this medium sounded amenable, the talks have broken down repeatedly.

CONCLUSION

Cyber security management in India is a complicated process. It requires both technological expertise and legal compliances. Some developed nations have enacted cyber security regulations but they have outlived their natural lives. The present day cyber security regulations require a techno legal orientation that is a big challenged for legislators around the world. India has enacted the information technology act, 2000 that governs legal issues of e- commerce, e-governance, cyber crimes, etc. However, techno legal experts believe that Indian laws like IT Act 2000 and telegraph act require urgent repeal and new and better techno legal laws must be enacted to replaces these laws. There are no dedicated cyber security laws in India. Indian government has drafted the cyber security policy of India 2013 but the same has not been implemented so far. Further, the policy is also suffering from many shortcomings including lack of privacy and civil liberties protection and absence of cyber security breaches disclosure norms. The cyber security trends of India have also shown poor cyber security preparedness of India to protect its cyberspace and critical infrastructures.

India has still to take care of issues like critical infrastructure protection, cyber warfare policy, cyber terrorism, cyber espionage, e-governance cyber security, e- commerce cyber security, cyber security of banks, etc. Companies and individuals are also required to cyber insure their businesses from cyber threats. Indian government is in the process of formulating a cyber crime prevention strategy. This has come in the wake of a public interest litigation (PIL) filed at the Supreme Court of India that has asked the centre to frame regulations and guidelines for effective investigation of cyber crimes in India. Simultaneously, the cyber crime investigation trainings in India are also needed.

In today's information age, Internet is the engine for global economic growth and the cyber security initiatives of any country should not impede it. Cyber security must be considered as a key enabler for India's economic growth and the government and industry efforts/initiatives should reflect this realization. To establish itself as the knowledge hub of the world, the key imperative for India is to address the cyber security challenges by leveraging the strengths of public and private sectors through public-private partnerships, considering the issue of cyber security at the board level within organisations and taking leadership and partnering with other nations for addressing global concerns in cyber security.

REFERENCE:

1. Albert Marcella & Greenfield, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2nd ed., Auerbach Publications, Taylor & Francis Group,UK, 2018.
2. Alistair Kelman, Electronic Commerce - Law and Practice, Sweet & Maxwell, London, 2016.
3. Chris Reed, Internet law, Universal Law Publishing Co. Pvt. Ltd., Delhi, 2014.
4. Dr. Vishwanath Paranjape, Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India, Central Law Agency Publication, 2010.
5. F. Lawrence Street and Mark P. Grant, Law of the internet, LexisNexis Matthew Bender, New York, 2018.
6. Gregory J. Battersby, Charles W. Grimes, and Leonard T. Nuara, Drafting internet agreements, Wolter

Kluwer (India) Pvt. Ltd., New Delhi, 2010.
7. Heather Ann Forrest, Protection of geographic names in international law and domain name systems policy, Kluwer Law International, Netherlands, 2017.
8. Ian Walden, Chap. 9,"Computer Crime" in Chris Reed (Ed.), Computer Law, 3rd Ed. Oxford University Press, 2017.
9. J. F. Dunnigan, The Next War Zone: Confronting the Global threat of Cyberterrorism. New York: Citadel Press, 2003.
10. Loader Brian and Thomas Douglas, Cyber-Crime Law Enforcement, Security and Surveillance in the Information Age, Routledge Publication, London, 2000.
11. Nandan Kamath, Law Relating to Computers, Internet and E- commerce: A Guide to Cyber Laws and the Information Technology Act, 2000, Universal Law Publishing Co., 2012.
12. Pedro Letai, Cyber law in Spain, Kluwer Law International, Netherlands, 2014.
13. Tyson Macaulay, Critical Infrastructure: What, Who Cares, and Why, Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies, CRC Press, Florida, 2018.
14. Uta Kohl, Juridiction and the internet, Cambridge University Press, Cambridge, U.K. 2007.
15. Vivek Sood, Cyber Crimes, Electronic Evidence and Investigation: Legal Issues, Nabhi Publication, Bangalore, 2010.
16. W. L. Simon, The Art of Deception: Controlling the Human Element of Security, Wiley Publishing, 2018.
17. Walter B. Wriston, The Twilight of Sovereignty - How the Information Technology Revolution is Transforming Our World, Maxwell Macmillan International, New York, 2014.