An Overview of Cyber Security in India

[1]Dr. Mamta Bansal
[1,]Shobhit Institute of Engineering and Technology (Deemed to be University), Meerut
Email Id- [1]mamta.bansal@shobhituniversity.ac.in

ABSTRACT: In the Information, Communication, and Technology (ICT) era, cybersecurity has evolved into a complex and fast-moving security issue (ICT). As the world's reliance on ICT grows, cyberthreats appear likely to infiltrate every nook and cranny of national economies and infrastructure; indeed, the growing reliance on computers and Web networking has been accompanied by a rise in cyberattack incidents targeting individuals, business owners, and governments around the world. Meanwhile, some countries are increasingly seeing ICT as both a strategic asset to be utilized for national security and a battlefield on which strategic battles may be waged. This article analyzes the importance of cybersecurity in today's security discussion, expanding on the analysis by looking at cybersecurity from India's viewpoint. The need of a cyber-security architecture to safeguard the growing ICT infrastructure in today's information society cannot be overstated. ICT infrastructure is the common thread that connects all important national infrastructures. All E-governance and E-commerce activities being undertaken across the globe need the presence of a reliable cyber security infrastructure. In this article, an attempt is made to provide a glimpse of this infrastructure, as well as anticipated patterns and imperatives that emerge from this research in the context of India.

KEYWORDS: Vulnerability of ICT infrastructure, Regulatory framework for ICT infrastructure, cyber security standards, Next Generation Networks, e-governance.

1. INTRODUCTION

In India, policymakers have paid relatively little attention to cybersecurity, to the point where the government has been unable to address the country's growing need for a robust cybersecurity apparatus. In summary, India lacks strong offensive and defensive cybersecurity skills, which is compounded by a lack of access to critical mechanisms for combating advanced malware such as Stunt , Flame, and Black Shades [1]. Furthermore, in comparison to other developed countries, India has far fewer cybersecurity projects and initiatives. Many of the pertinent initiatives planned by the Indian government have simply existed on paper. Furthermore, authorized initiatives such as India's National Critical Information Infrastructure Protection Centre (NCIPC) and National Cyber Coordination Centre (NCCC) have yet to come to fruition. Worse, India's 2013 National Cyber Security Policy has failed to produce positive results, as its implementation appears to be lacking in a number of areas, including privacy violations in general and civil liberties intrusion in particular. At the same time, India must protect critical infrastructure from cyberattacks, including banks, satellites, automated power grids, and thermal power plants. Indeed, the Indian government has acknowledged that there has been a significant increase in cyberattacks on financial services and banking institutions.

Viruses, hacking, identity theft, spamming, email-bombing, online defacement, cyber defamation, and denial of service have all been reported over the Internet in India [2]. For example, despite being ranked 85th in the world in terms of internet connectivity, the country ranks seventh in terms of cyberattacks. Surprisingly, cyberattacks increased from 23 in 2004 to 62,000 by mid-2014 [3]. Cyberthreats and assaults against government institutions increased by 136 percent in 2013, while efforts against Indian financial services companies increased by 126 percent. Large businesses have been the target of 69 percent of attacks (IANS 2014). Finally, four out of ten attacks in 2014 were carried out on nontraditional services industries such as business, hospitality, and personal services, according to a report by security software maker Symantec [2]. As a result, India must develop an effective cybercrisis management plan in order to address these and other similar challenges. In India, the IT industry has emerged as one of the most important drivers of economic development, as well as an essential component of the country's business and government. The industry has a beneficial impact on Indian people' lives by contributing directly or indirectly to the development of many socio-economic criteria such as living standards, employment, and diversity. Furthermore, information technology has played a critical part in converting India into a worldwide leader in business services and world-class technological solutions [4].

Simultaneously, the expansion of the IT industry has brought with it a huge and growing demand to protect the computing environment, as well as the requirement to create sufficient confidence and trust in this sector [5]. Most financial institutions and the banking industry, for example, have integrated IT into their operations, opening up countless opportunities for growth while also making these institutions vulnerable to cyberattacks in their daily operations, making the apparent lack of strategies to deal with these types of threats particularly concerning (Jain 2014). The government, for its part, has aided increased adoption of IT-enabled services and programs, such as the Unique Identification Development Authority of India (UIDAI) and the National e-Governance Programs, by establishing a large-scale IT infrastructure and encouraging corporate participation. Computer networks are now extensively used in critical sectors such as defense, banking, energy, telecommunications, transportation, and other public services to transmit data for commercial transactions as well as a source of information and communication. To date, the government has ambitious ambitions to expand ecommerce services, improve cyber connection, and improve the use of IT in communications in general. “The cabinet has approved the ambitious ‘Digital India' project that seeks to link all gram panchayats with broadband internet, promote e-governance, and turn India into a connected knowledge economy,” said Indian Prime Minister Narendra Modi. All of this government investment in new technology necessitates the establishment of strong regulations to ensure that these industries are secure.

A growing dependence on technology has rendered the systems that serve India's vital defense and intelligence communities susceptible to cyberattacks. Indeed, assaults on government equipment raise the risk of military and state secrets being stolen. As a result, it's not unexpected that many organizations within the Indian Ministry of Defense have taken on the task of dealing with cybersecurity. The Indian Army, for example, established the Cyber Security Establishment in 2005 to safeguard the army's networks at the division level and perform secure cybersecurity assessments (Pandit 2005). In addition, the army built a cybersecurity lab at the Military College of Telecommunications Engineering in Madhya Pradesh in 2010 with the goal of providing officers with specialized training in security procedures for the army's signal and data transmission networks (Governance Now 2010). The Indian Ministry of Communications and Information Technology published a draft National Cybersecurity Policy in March 2011, with an emphasis on critical infrastructure security and protection, development initiatives, and public-private partnerships (DEITY 2012). Under the aegis of the National Security Council, a proposal to establish the National Critical Information Infrastructure Protection Centre in accordance with the draft policy was prepared in June 2012. With the help of national and sector-specific Computer Emergency Response Teams (CERTs), the goal was to guarantee the protection of the state's vital infrastructure (Joseph 2012). In May of the same year, the Defense Research and Development Organization developed an indigenous cyber defense system to guarantee the safety and security of network sectors. As of May 2012, the project was said to be approximately half-completed (UNIDIR 2012). Around the same time, the Technical Intelligence Communication Centre and the National Defense Intelligence Agency formed a joint team to increase awareness about possible cyber vulnerabilities inside the government (Singh and Philip 2010). Critical infrastructures (such as banking and finance, energy, communication, commerce, health care, and transportation) are critical to modern society, and their failure to meet an expected service level could have a significant impact.

Infrastructures that were previously independent are becoming entangled in a network-of-networks. Information and communication technologies play a critical role in this interconnection. The following paragraph from President George W. Bush's executive order of October 16, 2001, summarizes the key issue in the aftermath of the 9/11 attack on the World Trade Center in New York. The information technology revolution has altered how business is conducted, government functions, and national defense is carried out. These three functions are now reliant on a network of interconnected critical information infrastructures. The protection program authorized by this order will include ongoing efforts to secure critical infrastructure information systems, including emergency preparedness communications, as well as the physical assets that support them. Telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services all rely on the security of these systems. When infrastructures are linked, new vulnerabilities can emerge from shared links, failures can spread across systems, and intrusion and disruption in one infrastructure can lead to unexpected threats in others. In such situations, it is critical to specify dependability and trust requirements and translate them into performance and functionality requirements for other systems. Cooperation and coordination among countries appear to be essential at the regional and international levels when using a comprehensive approach. A national strategy for cyber security and critical information infrastructure protection would include the development of legal frameworks to combat cybercrime, according to a regional workshop on cyber security and critical infrastructure protection held in Hanoi in August 2007 under the auspices of the International Telecommunication Union (ITU 2007). Because of its complexity, many researchers agree that infrastructure is its own worst enemy (Eeten et al, 2006). Because of the increased use of ICTs and increased functional demands, it is futile to attempt to maintain a separation of systems, each with its own internally delineated mode of responsibility. The line between inside and outside the system, as well as the concept of system boundaries as a whole, blurs.

1.1 Cybersecurity challenges in India:

- *Devices used for internet access are not uniform*: Not everyone in India can afford expensive phones because of the various income groups. Apple has a market share of over 44% in the United States. In India, however, iPhones are used by less than 1% of mobile users due to their higher security standards. The widening security gap between the high-end iPhone and lower-cost smartphones makes it nearly impossible for regulators to set legal and technical data protection standards.
- *Cybersecurity architecture at the national level is lacking*: critical infrastructure is owned by the private sector, and the military has its own firefighting agencies. However, there is no national security architecture that unifies all of these agencies' efforts to assess the nature of any threat and effectively counter it. The Prime Minister's Office has established a position dedicated to this cause, but India still has a long way to go before it has the necessary infrastructure.
- *Lack of separation*: Unlike countries or states, cyberspace has no borders, leaving the armed forces, ONGC's digital assets, banking functions, and other functions vulnerable to cyber-attacks from anywhere. This could lead to national security breaches, resulting in the loss of money, property, or lives. To respond to potential threats to the country's most valuable resources, a technically equipped multi-agency organization is required, one that can make decisions based on policy inputs and a sound strategy.
- *Lack of awareness*: Because there is no national cybersecurity policy in place, there is a lack of awareness at both the corporate and individual levels. Only a guided and supervised legal framework can protect and be protected domestic netizens from cyber-attacks.

1.2 Initiatives at International level:

Several international governance and security organizations, like the United Nations (UN), the Organization for Economic Cooperation and Development (OECD), and the North Atlantic Treaty Organization (NATO), are paying close attention to cyber security (NATO). Despite this focus, there is currently no one worldwide regulatory agency tasked only with combating cybercrime. Instead, several of these organizations' subordinate organizations, such as the United Nations' International Telecommunication Union (ITU), have turned their attention to this problem (Nain et al, 2007). The United Nations General Assembly passed Resolution 56/183 in 2001, calling for the creation of a World Summit on the Information Society (WSIS), where public and private sectors could "...harness synergies and create cooperation among the various information and communication technologies initiatives, at the regional and global levels." (2002, ITU/WSIS) The Information Telecommunication Union (ITU) was chosen to act as the Summit's manager. The World Summit was held in two parts, one in Geneva in December 2003 and the other in Tunis in November 2005. The Geneva phase's goal was to create and nurture a clear declaration of political intent, as well as a strategy for the foundations of a "...Information Society for All..." and a broad plan of action. (World Summit on the Information Society, 2006) Following the conference, two main themes emerged building confidence, trust, and security and stablishing solid regulatory frameworks. (World Summit on the Information Society, 2006) Each summit generated reports, the most recent of which was released in June 2007.

The United Nations Group on Information Society (UNGIS) was established in 2006 to coordinate the UN's activities in response to the WSIS results. “UNGIS is a UN system-wide interagency coordination mechanism for putting WSIS's findings into action. The Group facilitates synergies aimed at resolving substantive and policy problems, eliminating redundancies, and improving system effectiveness while increasing public knowledge of the global Information Society's aims and objectives. UNGIS also strives to emphasize the significance of information and communication technologies (ICTs) in achieving the “Millennium Development Goals.” UNGIS' goals include facilitating synergies across UN system institutions in order to optimize collaborative efforts, avoiding duplication and increasing effectiveness in attaining WSIS results, and raising public knowledge of the UN system's implementation of WSIS. 2007 (UNGIS) Security issues have been more important in the development and use of Information Systems (IS) in both the public and commercial sectors during the past two decades. Many industries and companies are still feeling the heat, with particular laws requiring sophisticated security Risk Management (RM) procedures. This is the case, for example, in the United States with the Sarbanes-Oxley Act, which addresses the integrity of financial and accounting data, or in the banking industry with the new Basel II agreement, which establishes rules for determining the level of “frozen” capital for financial institutions based on the maturity of their RM activities, including those related to there is countries have enacted safeguards in the form of laws and guidelines. The United States and the United Kingdom have well-defined and extensive data security and privacy legislation. At the federal and state levels, the United States has sector-specific legislation. The United Kingdom has a comprehensive Data Protection Act that applies to all industries [6].

1.3 Initiatives taken in Indian Context:

In the 1990s, the country began a phase of economic liberalization. To attract foreign investment, one of the major aspects of this approach has been to simplify laws and regulations. As a consequence, India is becoming more accessible from a legislative and economic standpoint, but there are still challenges to be addressed, one of which is Indian privacy requirements for outsourcing firms. Although India lacks explicit rules on privacy and data protection, proxy laws and other indirect protections exist that offer sufficient protection to businesses who outsource services [7]. The Indian IT Act, in combination with other relevant legislation, provides a fundamental legal framework. As outsourcing becomes more common and the market becomes more competitive, the ability to demonstrate the presence and ongoing usage of strong protections will become one of the most important considerations for businesses choosing which provider to partner with [8]. On August 29, 2005, the Ministry of Information Technology proposed certain amendments to the Indian Information Technology Act 2000, as shown in Figure 3. The Information Technology (Amendment) Act of 2006 included these changes. The Government of India strategically decided to take effective steps for the creation of the National Informatics Centre (NIC), which has been instrumental in steering information and communication technology (ICT) applications in government departments at the center, states, and districts, facilitating improvements in government services, wider transparency in government functions, and improvements in decennial [9].The Department of Electronics (DOE), the National Informatics Centre (NIC), and the Technology and Software Export Development Council were merged into a new Ministry of Information Technology (MIT) in 1999. In the same year, the New Telecom Policy (NTP) was launched, providing a much-needed policy framework. The Department of Telecommunication (DOT) was later merged with MIT to form the Ministry of Communication and Information Technology, in recognition of the convergence of IT and telecommunication. The Telecom Regulatory Authority of India (TRAI) and Telecom Dispute Settlement and Appellate Tribunal (TDSAT) were established in 1997 and 2000, respectively, to provide regulatory framework for India's rapidly evolving telecommunication infrastructure. NIC has created a project center at National Informatics Centre Network (NICNET) nodes to tailor programs for decision assistance in development and responsive administration. In the field of E-governance, NIC conducts IT initiatives in cooperation with the federal and state governments. The NIC's cyber security group is in charge of the cyber security of the ICT infrastructure being built for E-governance. However, there are no information on the NIC website [10].

2. DISCUSSION

Despite its international reputation as an information technology superpower, India is far behind when it comes to the official cyber security workforce, which only numbers a few hundred people. A large number of experts working for various government agencies Cyber security is quickly becoming an essential component of any business. Security of information This can be deduced from the current situation. According to a research, as the incidence of cybercrime rises, more people are becoming victims. detection techniques, as well as educating users on how to be safe It is necessary to establish a safe online environment with complete guidance. To be aware of the advantages and disadvantages of the internet before using it. Insider threats are one of today's most serious security concerns. threat. Lack of consistency is another major security concern. when it comes to enforcing the "acceptable use" policy. Measurements that are specific In order to hunt down electronic evidence, you'll need to find it. They should be preserved so that systems are better protected. Intrusions into the computer network in order to protect against cybercrime and intrusion, Techniques for detection should be devised, implemented, and evaluated. Administrated. For the time being, the best way to protect it would be for everyone to do their part. to think ahead and take preventative measures Individuals, these should be followed by all institutions and governments measures.

3. CONCLUSION

Our vulnerability to harm from natural disasters or attacks by insurgents/terrorists with the goal of immobilizing and paralyzing the nation's day-to-day activities is growing as our investments in ICT infrastructure grow. Such damage would result in a short- and long-term economic setback. While planning and implementing India's ICT infrastructure, we can learn a lot from the US initiative to secure our cyber system. Natural or insurgency/terrorist-caused disasters put an exponential amount of strain on available ICT systems, which must facilitate coordination between various agencies such as fire departments, medical services, police, the media, and the civil administration. It is proposed that the nation's existing and planned ICT infrastructure, both public and private, be analyzed by a group of experts under the auspices of the NDMA, with the goal of recommending appropriate operational arrangements to reduce vulnerability to perceived attacks by hostile elements and natural disasters. This would necessitate a detailed technical examination of current and future wireless and wired ICT systems. The expert group should identify and recommend an appropriate mix of redundancies in the critical ICT systems that support the nation's governance structure. A focused analysis of security flaws and their protection would lead to recommendations that would avoid duplication of effort and, as a result, be more cost-effective at the national level. It would be condescending to believe that technological and scientific capabilities alone can completely control disasters. The most sacred component of any such venture is the participation of all stakeholders in order to ensure an appropriate solution for humanity's welfare.

REFERENCES

[1] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *Comput. Secur.*, 2013, doi: 10.1016/j.cose.2013.04.004.

[2] T. Limba, T. Plėta, K. Agafonov, and M. Damkus, "Cyber security management model for critical infrastructure," *Entrep. Sustain. Issues*, 2017, doi: 10.9770/jesi.2017.4.4(12).

[3] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cyber security investment," *Decis. Support Syst.*, 2016, doi: 10.1016/j.dss.2016.02.012.

[4] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Computers and Security*. 2016, doi: 10.1016/j.cose.2015.09.009.

[5] T. Limba, K. Agafonov, L. Paukštė, M. Damkus, and T. Plėta, "Peculiarities of cyber security management in the process of internet voting implementation," *Entrep. Sustain. Issues*, 2017, doi: 10.9770/jesi.2017.5.2(15).

[6] F. Smith and G. Ingram, "Organising cyber security in Australia and beyond," *Aust. J. Int. Aff.*, 2017, doi: 10.1080/10357718.2017.1320972.

[7] P. Saxena, B. Kotiyal, and R. H. Goudar, "A Cyber Era Approach for Building Awareness in Cyber Security for Educational System in India," *Int. J. Inf. Educ. Technol.*, 2012, doi: 10.7763/ijiet.2012.v2.102.

[8] N. Singh and A. Rishi, “Pyramid: A case study of cyber security in India,” *South Asian J. Bus. Manag. Cases*, 2015, doi: 10.1177/2277977915574046.

[9] V. Ananda Kumar, K. K. Pandey, and D. K. Punia, “Cyber security threats in the power sector: Need for a domain specific regulatory framework in India,” *Energy Policy*, 2014, doi: 10.1016/j.enpol.2013.10.025.

[10] F. Cassim, “Addressing the spectre of cyber terrorism: a comparative perspective,” *Potchefstroom Electron. Law Journal/Potchefstroomse Elektron. Regsbl.*, 2017, doi: 10.17159/1727-3781/2012/v15i2a2494.