International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 1, November-December 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cyber Security Challenges and Emerging Trends

Dr. S. Krishnan[1], Yogesh Kalla[2]

[1]Associate Professor, [2]Student of BA LLB (Hons),
[1,2]Seedling School of Law and Governance, Jaipur National University, Jaipur, Rajasthan, India

ABSTRACT

Cyber security plays an important role in the field of Information Communication and Technology. Securing information have become the major challenges in the present day. As the dependence on ICT is deepening across the globe, cyber threats appear likely to penetrate every nook and corner of national economies and infrastructure; indeed, the growing dependence on computers and Internet-based networking has been accompanied by increased cyber-attack incidents around the world, targeting individuals, businesses, and governments. Meanwhile, ICT is increasingly being seen by some governments as both a strategic asset to be exploited for the purposes of national security and as a battlefield where strategic conflicts can be fought. This paper examines the primacy of cyber-security in the contemporary security debate, deepening the analysis by looking at the domain of cyber-security from the perspective of India.

KEYWORDS: *Cybersecurity, Information Technology, cyber threats, cybercrime*

How to cite this paper: Dr. S. Krishnan | Yogesh Kalla "Cyber Security Challenges and Emerging Trends" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-1, December 2021, pp.842-849, URL: www.ijtsrd.com/papers/ijtsrd47939.pdf

IJTSRD47939

INTRODUCTION

The concept of security is a core concept in the study of international relations. Traditionally, and until relatively recently, security analysis focused on state security, viewing it as a function of the levels of threats which states face from other states, as well as the manner and effectiveness of state responses to such threats (Rather and Jose 2014). However, after the end of the Cold War, scholars shifted focus from the state-centric notion of security, enlarging the concept to include the protection of the individual (Buzan 1991). At approximately the same time, the nature of threats changed from external aggression to intra-state conflicts arising due to civil wars, environmental degradation, economic deprivation, and human rights violation. It is in this context that national security came to include within its ambit other issues of security apart from territorial protection, such as poverty, industrial competitiveness, educational crises, environmental hazards, drug and human trafficking, and resource shortages. Finally, the recent Information, Communication and Technology (ICT) revolution — including the Internet, email, social websites, and satellite communications — has revolutionised every aspect of human life, posing new challenges to national security.

Attributable to amazingly powerful web speeds, cyber protection is one of the world's most squeezing needs, as cyber-attacks represent a critical danger to a nation's security. Individuals ought to be educated about how to overhaul their organization's security designs and gadgets, just as how to utilize appropriate enemy of infection programming with the goal that their organizations are malware and infection-free.

Indeed, in the digital age, the arena of the national security is confronted with previously unfamiliar threats aimed at destroying a state's technology infrastructure. It is an obvious truism that, in the globalized world, the Internet and ICTs are essential for economic and social development, forming a vital digital infrastructure upon which societies, economies, and governments rely to perform their essential functions. The relatively open nature of the Internet guarantees that it is, on numerous levels, an unsafe environment (Pillai 2012). As such, cybersecurity has come to encompass a wide range of issues such as critical infrastructure protection,

cyberterrorism, cyberthreats, privacy issues, cybercrime, and cyberwarfare.

Securing networks, files, services, and other information from unsupervised or unapproved users, alteration, or destruction is the most basic concept of cyber security. Because of recent cyber-attacks all over the world, cyber security is becoming increasingly important. Many businesses create data security tools. It alludes to the protections set up to hold information back from being taken, hacked, or focused on.

Various layers of safeguard through PCs, machines, organizations, and projects make up a decent network protection system. Then again, a powerful network safety system doesn't depend entirely on cyber defense technology; it likewise comes down to individuals settling on wise digital safeguard choices.

The essential objective of the innovation created by organizations is to defend the information in their frameworks. Cyber security not only ensures safe data but also prevents virus attacks. After the United States and China, India has the third-largest number of internet users.

In the second decade of the twenty-first century, cyberthreats are evolving and increasing at a fast pace. They are still initiated by criminal actors but also come from new sources, such as foreign states and political groups, and may have motivations other than money making. These latter may include some types of "hacktivism" in the name of a political cause, political destabilisation (e.g., Estonia in 2007), cyberespionage, sabotage (e.g., Stuxnet), and even military operations (OECD 2012, 12). The sophistication of cybercriminals, the emergence of cyberespionage, as well as the well-publicised activities of hacker collectives have combined to create the impression that cyberattacks are becoming more organised and that the degree of sophistication has increased significantly, showing clear signs of professionalisation.

Given this backdrop, states have increasingly recognized cybersecurity as a top security issue, one that will only grow in importance as time goes on (Cavelty 2012). At the same time, cybersecurity has emerged as a national policy priority to be approached in a holistic manner, encompassing economic, social, educational, legal, law-enforcement, technical, diplomatic, military, and intelligence-related aspects. "Sovereignty considerations" have become increasingly important

Types of cyber security

It's essential to analyze forms of cyber security in order to be properly secured-

Critical infrastructure security- The need to defend a country's fundamental framework, like food and farming or transportation, is known as critical infrastructure protection (CIP). Each administration in each nation is liable for shielding these crucial framework resources from catastrophic events, fear-monger assaults, and, increasing cyber dangers. Critical infrastructure organizations should have a strong framework set up that can foresee and forestall disaster through their whole basic framework setting.

Network security- In its most fundamental structure, it is an assortment of decides and conventions that utilization both programming and equipment innovation to ensure the security, privacy, and availability of PC organizations and information. Any business, paying little mind to its scale, area, or framework, needs network safety efforts to defend itself from the ever-increasing spectrum of cyber threats that exist today. Network security can deal with network traffic all the more successfully, improve network solidness, and guarantee safe information trade among representatives and information sources as well as ensuring resources and the respectability of information from outside abuses.

Application security- Application security is the way of forming, integrating, and evaluating security features into applications to shield them from threats like illegal disclosure and alteration. Application security alludes to security steps taken at the application level to stay away from the robbery or seizing of information or code inside the product. It includes security suggestions made during application examination and execution, as well as frameworks and methods for protecting apps after they've been released.

Information security- Information security, or infosec, is centered on forestalling unapproved admittance to frameworks. It is a part of information hazards the executives that involve halting or decline the chance of unapproved entry, usage, leakage, interruption, elimination, abuse, alteration, inspection, or recording. Information security specialists are dynamic in handling the reasons for a security incident if one occurs. Remember that information might be electronic, physical, or immaterial.

Cloud security- Cloud security, also referred to as cloud computing security, is a collection of plans, regulations, protocols, and innovations which function together just to safeguard cloud-based applications, data, and networks. One of the benefits of utilizing cloud storage and encryption is that it eliminates the need for dedicated equipment. Not exclusively will this get a good deal on capital, but it also saves money on operating costs. While

previously, IT groups needed to manage security issues as they emerged, cloud security gives proactive security capacities that give protection 24/7.

Data loss prevention- The word "data leakage protection" applies to protecting organizations against security breaches and leaks. A ransom ware attack, for example, is an illustration of information misfortune. The aim of data loss prevention is to safeguard information from being transferred outside of the organization. Establishing a DLP technique will uncover how information is utilized by partners. To get secret data, organizations should initially comprehend what it is, the place where it is kept, who utilizes it, and why. Organization used it for protect Intellectual Property critical for the organization.

End-user education- Perceives that digital insurance programs are similarly pretty much as great as individuals who use them. End-user education entails instructing clients on prescribed procedures, for example, not tapping on obscure connections or opening dubious attachments in emails, all of which may empower malware and other noxious programming to penetrate the framework. Once installed, it awards admittance to the end client's PC, which is utilized as a dispatch point for get-together organization information and growing organization control. On account of the genuine outcomes, it's significant that end clients comprehend the most mainstream techniques that cyber criminals compromise them.

Scale of cyber security threats

Viruses used during cyber-attacks include malware, spyware, ransomware, fraud, phishing, and others. When a computer user has clicked on compromised web pages, links, malicious websites, or unwittingly downloads harmful software, attackers can easily grant access to that person's computer networks. Cyber security is critical in avoiding some of the most difficult and egregious crimes, such as blackmail, fraudulent purchases from another account, and confidential data leakage.

It's vital to comprehend the three types of network safety dangers: cyber-crime, cyber-attacks, and cyber-terrorism in order to better secure yourself.

- One or more people perpetrate cybercrime against your framework to make interruption or accomplish monetary benefit.
- **Cyber attacks** are frequently done for political purposes and they might be proposed to catch and spread private information.
- **Cyber terrorism** is a type of psychological warfare that includes breaking into electronic organizations to cause frenzy and dread among its objectives.

Cyber Security Techniques:

Cyber-attacks on cyberspace can grow by capitalizing on new techniques. Cybercriminals will most frequently change the current malware signatures to take advantage of new technical faults. In other instances, they actually search for special features of emerging technology to detect weaknesses in malware injection. Cyber criminals are taking advantage of emerging Internet technology and millions and billions of active users to access a huge amount of people easily and effectively using these new technologies.

Access Control and Password Security: Security provided by the means of username and password is a simple way of providing security for the private information to preserve privacy. This means of providing security is one of the most critical cyber security initiatives.

Authentication of Data: Until the transmitted information need to be attested that it has come from a reputable supply that was not changed. These documents are often authenticated using a gift from the opposing virus software package inside computers. An honestly opposed virus software package is more essential to protect devices from viruses.

Malware Scanners: A software system which sometimes scans all files and documents for malicious code or harmful viruses inside the system. The samples of malicious software systems in this field are generally sorting and noted as malware by viruses, worms, and the Trojan horses.

Firewall: Firewall is a software or hardware package which helps separate hackers, viruses and worms trying to access your PC through the web .The firewall checks all messages that come in and blocks those that fail to meet the security requirements compatible with all messages .Firewalls plays a very vital role in malware detection.

Role of Social Media in Cyber Security: In recent modern world, there is a need of interactive businesses which needs to find new ways to secure personal information in more entangled environment. Social media has important role to play in cyber security and in personal cyber-attacks. Adoption of social media among employees is growing and threat of attack is therefore increasing since most of them nearly use social media or social networking sites everyday it is now a massive forum for cyber criminals to hack private information and steal valued information. In recent days, it's very easy to share

personal information easily and businesses must make sure that recognise, react in real time and prevent breaches of any kind as quickly as possible. These social media has easily make people to share their private information and hackers can use these information. Therefore, people have to take reasonable steps to avoid misuse and loss of their information through these social media.

Cybersecurity in India: Background

In the Indian context, the issue of cybersecurity has received relatively little attention from policymakers, to the extent that the government has been unable to tackle the country's growing needs for a robust cybersecurity apparatus. In short, India lacks effective offensive and defensive cybersecurity capabilities, exacerbated by the lack of access to mechanisms vital to confronting sophisticated malware like Stuxnet, Flame, and Black shades (Kaushik 2014). Moreover, cybersecurity projects and initiatives in India are far fewer in number as compared to other developed nations. Many of the relevant projects proposed by the Indian government have remained on paper only. In addition, approved projects like the National Critical Information Infrastructure Protection Centre (NCIPC) and National Cyber Coordination Centre (NCCC) of India have failed so far to materialize. Worse, the 2013 National Cyber Security Policy of India has failed to bear fruitful results, as its implementation seems to be weak in numerous aspects, including privacy violation in general and intrusion into civil liberties in particular.

At the same time, India faces a vital need to protect critical infrastructures such as banks, satellites, automated power grids, and thermal power plants from cyberattacks (Kaushik 2014). Indeed, the Indian government has admitted that there has been a large spike in cyberattacks against establishments such as the banking and financial services sector. Malicious activity on the Internet in India has ranged from viruses, hacking, identity theft, spamming, email-bombing, web defacement, cyber defamation, to the denial of service.

For example, even though the country ranks eighty-fifth in net connectivity compared to other countries globally, it holds the seventh spot in terms of cyberattacks (Express News Service 2014). Strikingly, the number of cyberattacks rose from 23 in 2004 to 62,000 by mid2014 (The Economic Times 2014a). The year 2013 alone saw a 136 percent increase in cyberthreats and attacks against government organizations as well as a 126 percent increase in attempts against Indian financial services organizations (Athavale 2014). Approximately 69 percent of attacks have targeted large enterprises (IANS 2014). Finally, according to a report by security software-maker Symantec, four out of ten attacks in 2014 were carried out on nontraditional services industries like business, hospitality, and personal services (Indo-Asian News Service 2014). A clear need, therefore, exists for India to develop an effective cybercrisis management plan, in order to address these and similar challenges.

Cyber Security in India:

In-Depth The IT sector in India has emerged as one of the most significant catalysts for the country's economic growth, and as an integral part of the country's business and governance. The sector is positively influencing the lives of Indian citizens through direct or indirect contribution to the improvement of several socio-economic parameters, such as the standard of living, employment, and diversity. In addition, IT has played a key role in transforming India into a global player in providing business services as well as world-class technology solutions (DEITY 2011).

At the same time, the growth of the IT sphere has been accompanied by a tremendous and increasing need to secure the computing environment, as well as the necessity to build adequate confidence and trust in this sector (DEITY 2012). For example, most financial institutions as well as the banking industry have incorporated IT in their operations, opening up countless opportunities for growth while at the same time making these institutions vulnerable to cyberattacks in their daily activities and making the evident absence of strategies to deal with these types of threats particularly worrisome (Jain 2014).

For its part, the governmental sector has facilitated the increased adoption of IT-enabled services and programs, such as the Unique Identification Development Authority of India (UIDAI) and National e-Governance Programs (NeGP), creating a large-scale IT infrastructure and promoting corporate participation. Critical areas such as defence, finance, energy, telecommunication, transport, and other public services currently heavily depend on computer networks to relay data for commercial transactions as well as a source of information and for communication purposes. To date, the government has ambitious plans to further raise ecommerce services, cyber connectivity, and to generally enhance the use of IT in communications. Indian Prime Minister Narendra Modi's statement that "the cabinet has approved the ambitious 'Digital India' programme that aims to connect all gram panchayats by broadband internet, promote e-governance and transform India into a connected knowledge economy" is typical in this regard (The Economic

Times 2014b). All of this governmental investment in the new technologies militates for the adoption of strong policies to provide robust security to these sectors (Verma and Sharma 2014).

Particularly worthy of note, an increased reliance on IT has made the systems supporting India's critical defence and intelligence community vulnerable to cyberattacks. Indeed, attacks on government machinery carry the increased threat of theft of military secrets and state secrets (Aiyengar 2010). Unsurprisingly, then, several organisations within the ambit of the Indian Ministry of Defence have taken on the responsibility of dealing with cybersecurity. For instance, in 2005 the Indian Army formed the Cyber Security Establishment to protect the army's networks at the division level as well as to conduct safe cybersecurity audits (Pandit 2005). Also, in 2010 the army established a cybersecurity laboratory at the Military College of Telecommunications Engineering in Madhya Pradesh, with a view to provide officers with specialised training in security protocols for its signal as well as data transmission networks (Governance Now 2010).

Energy and Cybersecurity

Securing the energy sector has emerged as a critical non-traditional security issue for India. The country ranks fourth in the world in terms of primary energy consumption; at the same time, the average level of consumption per capita is very low (TERI 2013). Due to insufficient regulation of information sharing and incomplete institutions to facilitate it, information on cyberattacks and equipment vulnerabilities in the Indian energy sector is nearly non-existent. But we can suppose from trends in international cybersecurity that the sector is increasingly targeted by the sophisticated attacks, particularly as India has embarked on linking it with modern technologies in order to meet growing energy needs (Walstrom 2016).

Indeed, with the advent of new technologies in this sector, several challenges began to appear on the scene. For instance, after India's nuclear test in May 1998, a group of hackers posted anti-India and anti-nuclear messages on the website of Bhabha Atomic Research Center (BARC) (Patil and Bhosale 2013). In addition, an online hacker called Phr OzenMyst hacked the official website of BARC and leaked some of its sensitive information; the attack was meant as a protest against ongoing government operations in the occupied part of Kashmir (The Pioneer 2013).

Furthermore, the critical infrastructure supporting every economic activity in India is fully dependent on the power sector; the dependence of this sector on ICT has highlighted several cybersecurity challenges. It is estimated that the period from 1994 to 2004 witnessed around 60 percent of all cyberattacks on the automatic power grids in India (Kumar et al. 2013). More recently, on July 30 and 31 2012, northern India witnessed a severe blackout that affected nearly 670 million people's normal life and work (Shuran et al. 2013), damaging all services in the region, including road traffic and railways. Chaos broke out on the roads as traffic lights and systems that supported them stopped working, with the police unable to cope with the situation. Simultaneously, there were reports of devastating fires and explosions in major refineries, with extensive damage and loss of life, all while pipelines were ruptured and oil flow was disrupted (IDSA 2012).

Defence and Cybersecurity

India has an extensive defence industrial base and maintains the third-largest armed forces in the world (KPMG 2010). At the same time, it has linked its defence sector with the new technologies, in the process opening the country up to a set of ever-evolving threats due to a dependence on these technologies and the reliance on integrating networks. For instance, in 2012 a cyberattack was launched by hackers against the Indian Navy's eastern command computer systems which oversee the testing of India's ballistic missile submarines and maritime activities in the South China Sea. The naval computers were infected by a virus that secretly collected confidential documents and files and transmitted them to Chinese IP addresses.

While Indian officials have yet to disclose the type of information that was targeted in this attack (Pubby 2012), the Navy is not the only Indian defence institution to have faced such adverse events — the National Security Agency (NSA) and the Air Force have proved to be vulnerable as well. In 2010 the hackers targeted the NSA's office as well as several computers of the Indian Air Force, opening up numerous small windows through which classified files and documents were stolen (Unnithan 2012). In the same year, the country witnessed the biggest cyberattack yet, in which more than 10,000 email addresses of the top government officials were hacked, particularly military officials, the Prime Minister's Office (PMO), defence, home ministries, external affairs, and intelligence agencies (Singh 2012).

Finance and Cybersecurity

India is one of the fastest growing economies in the world, with the adoption of IT acting as a catalyst behind this significant growth. But this reliance on IT has come at the cost of new vulnerabilities. It has generally been argued that the root cause of most

cyberattacks is monetary or financial gain (KPMG 2014). Indeed, the complexity of modern banking and financial services makes them vulnerable to cyberattacks from both state as well as non-state actors (Singh 2013). The interconnective nature of modern technologies has exacerbated the problem, creating widespread opportunities for fraud, theft, and other forms of exploitation (Bamrara et al. 2013). Recognizing this, former Indian Telecom Minister, Kapil Sibal has said that "cybersecurity is critical for economic security, and any failure to ensure cybersecurity will lead to economic destabilisation" (Singh 2013)

Over the past few years the financial sector in India has seen a rise in network security breaches, data losses, identity thefts, data thefts, and other white-collar crimes, causing the banking industry to incur huge losses, in amounts far exceeding conventional methods of bank robbery. For instance, in 2013 cyberattacks in India resulted in huge financial loses for Indian companies in the amount of nearly four billion dollars. A year later, financial losses from such attacks had increased by 30 percent. It is also estimated that India is among the world's top five countries in terms of incidence of cybercrime such as identity theft (11percent), ransomware (11 percent), and phishing (9 percent) (The Hindu 2013). In addition, the Reserve bank of India (RBI) has released data on commercial banks being targeted for the purpose of fraud, for example through Internet banking and ATM (debit/credit) cards. The number of such cases rose from approximately 4,049 lakhs in 2010 to 5267 lakhs in 2012 (Madaan 2013). In these circumstances, the need for India to develop a comprehensive cybersecurity strategy to fully guarantee protection for the financial sector becomes self-evident

What would you do to better defend yourself from cyber-attacks?

- Never open connections or associations in messages from obscure senders. Messages distinguished as sent by somebody you trust are perhaps the most mainstream ways for organizations and users to be exposed to malware and viruses.
- Just make sure your gadgets are up to date. Fundamental security fixes are remembered for programming refreshes. Digital hoodlums can likewise target old PCs that aren't running the most modern security programming.
- Back up your documents consistently for added security on account of a digital protection penetrate. On the off chance that you need to clean your PC off due to a cyber attack, having your records in a safe, separate area would help.

Conclusion

Cyber security is continually changing, making it hard to stay current. Remaining educated and practicing alert while utilizing the web is two of the best approaches to ensure yourself, your organizations and gadgets, and your business.

Cyberattacks targeting critical information infrastructures in India, such as energy, financial services, defence, and telecommunications, have the potential of adversely impacting upon the nation's economy and public safety. From the perspective of national security, the securing of the critical information infrastructure has become a top priority, in line with policies already adopted by other digital nations (DSCI 2013). Indeed, the ever-growing interdependence of the digital sphere, across borders, has provoked the emergence of cybersecurity as a major component of national security strategies in states across the globe (Kumar and Mukherjee 2013); India should not delay in following their example.

References

[1] Aiyengar, S. R. R. (2010). National Strategy for Cyberspace Security. New Delhi: KW Publisher.

[2] Athavale, D. (2014). "Cyberattacks on the Rise in India." The Times of India, Pune, March 10.

[3] Bamrara, A., G. Singh and M. Bhatt (2013). "Cyber Attacks and Defence Strategies in India: An Empirical Assessment of the Banking Sector." International Journal of Cyber Criminology, 7 (1): 49–61.

[4] Buzan, B. (1991). People, States, and Fear: An Agenda for International Security Studies in the Post Cold War Era. London: Harvester Wheatsheaf.

[5] Cavelty, M. D. (2012). "The Militarisation of Cyber Security as a Source of Global Tension." In Mockli, Daniel, Wenger, and Andreas, eds. Strategic Trends Analysis. Zurich: Center for Security Studies.

[6] Dilipraj, E. (2013). "India's Cyber Security 2013: A Review." Centre for Air Power Studies, 97 (14): 1–4.

[7] DSCI. (2013). Analysis of National Cyber Security Policy (NCSP–2013). New Delhi: Data Security Council of India.

[8] Gercke. (2009). Understanding Cybercrime: A Guide for Developing Countries, Geneva: ITU publication. Governance Now. (2010). Army

Sets Up Cyber Security Lab. http://www.governancenow.com/news/regular-story/army-sets-cyber-security-lab.
Government of India. (2011). Discussion Draft on National Cyber Security Policy. New Delhi: DIETY.

[9] Government of India. (2012). "National Telecom Policy (NTP) – 2012." Ministry of Communication and Information Technology (NTP). New Delhi, June 13.

[10] Government of India. (2012). National Cyber Security Strategy, India: DEITY. IANS. (2014). "69 Percent of Cyberattacks Targeted at Large Companies in India: Report." Business Standard, New Delhi, April 24.

[11] IDSA. (2012). India's Cyber Security Challenges. New Delhi: Institute of Defence Studies and Analyses.

[12] Indo-Asian News Services. (2014). "Large Firms Hit by 69 Percent of Targeted Cyberattacks in India: Symantec." April 26. http://gadgets/ndtv.com/internet/news/large-firms-hit-by-69-percent-oftargeted-cyber-attacks-in-india-symantec-513975.

[13] ITU. (2009). Series-X: Data Networks Open System Communication and Security, Overview of Cybersecurity ITU-T X.1205, Geneva: ITU.

[14] Jain, S. (2014). Cyber Security: A Sine Qua Non. http://www.indiandefencereview.com/news/cyber-security-a-sine-qua-non/.

[15] Joseph, J. (2012). "India to Add Muscle to Its Cyber Arsenal." Times of India, New Delhi, June 11.

[16] Kaushik, R. K. (2014). "Cyber Security Needs Urgent Attention of Indian Government." http://cybersecurityforindia.blogspot.in/2014/09/cyber-security-needs-urgent-attention.html.

[17] KPMG. (2010). Indian Defence Sector: The Improving Landscape for US Business and Indo-US Commercial, KPMG International, Swiss.

[18] KPMG. (2014). Forensic Technology Services: Cyber Crime Survey Report – 2014. KPMG International, Swiss.

[19] Kumar, A. V.; K. K. Pandey, and D. K. Punia (2013). Facing the Reality of Cyber-Threats in the Power Sector. Bangalore: Wipro Technologies.

[20] Kumar, R. & N. Mukherjee. (2013). Cyber Security in India: A Skill-Development Perspective. New Delhi: Communication Multimedia and Infrastructure.

[21] Madaan, N. (2013). "More in City Fall in Net Trap." Times of India, Pune, September 8.

[22] Manoharan, N. (2013). "India's Internal Security Situation: Threats and Responses." India Quarterly: A Journal of International Affairs 69 (4): 367–381.

[23] OECD. (2012). "Cybersecurity Policy Making at a Turning Point." http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf.

[24] Pandit, R. (2005). "Army Gearing Up for Cyberwarfare." Times of India, New Delhi, July 7.

[25] Patil, P. R. and Bhosale, D. V. (2013). "Need to Understand Cyber Crime"s Impact over National Security in India: A Case Study." Online International Interdisciplinary Research Journal 3 (4): 167–171.

[26] Pillai, P. (2012). "History of Internet Security." http://www.buzzle.com/articles/history-of-internet-security.html.

[27] Pubby, M. (2012). "China Hackers Enter Navy Computers, Plant Bug to Extract Sensitive Data." The Indian Express, New Delhi, July 1.

[28] Rather, M. A. & K. Jose (2014). "Human Security: Evolution and Conceptualization." European Academic Research, 2 (5): 6766–6797.

[29] Reddy, K. S. (2012). "Anonymous Takes Down MTNL Website." The Hindu, New Delhi, June 6.

[30] Reich, P. C., ed. (2012). Law, Policy, and Technology: Cyberterrorism, Information Warfare, and Internet Immobilization: Cyberterrorism, Information Warfare, and Internet Immobilization. IGI Global.

[31] Ruggiero, P. & J. Foote (2011). Cyber Threats to Mobile Phones. United State: US Department of Homeland Security. https://www.us-cert.gov/security-publications/cyber-threats-mobile-phones.

[32] Shuran, L., D. Hui, and G. Su. (2013). "Analyses and Discussions of the Blackout in Indian Power Grid." Energy Science and Technology 6 (1): 61–66.

[33] Singh, A. (2012). "Over 10,000 Email IDs Hit in 'Worst' Cyberattack." The Indian Express. New Delhi, December 18.

[34] Singh, H. and J. T. Philip (2010). "Spy Game: India Readies Cyber Army to Hack into Hostile Nations Computer Systems." Economic Times, New Delhi, August 6.

[35] Singh, S. (2013). "Cyber Security Plan to Cover Strategic, Military, Government and Business Assets." The Hindu, New Delhi, July 2.

[36] TERI. (2013). TERI Energy Data Directory & Yearbook (TEDDY) 2012/13. New Delhi: TERI Press.

[37] The Economic Times. (2012). "Indian OS Developed by DRDO Likely to Be Ready in Three Years." Hyderabad, December 20.

[38] The Economic Times. (2014). "Government Mulls Digital India Programme to Connect All Villages." New Delhi, August 21.

[39] The Economic Times. (2014). "Most Cyberattacks on India Show Chinese IP Address: NTRO." New Delhi, November 13.

[40] The Hindu (2013). "Cyber Frauds Cost India $4 Billion in 2013: Symantec." New Delhi, October 22.

[41] The Indian Express (2014). "Modi to Visit Australia after G-20 Summit." New Delhi, September 6.

[42] The Pioneer. (2013). "ECIL Website Hacked, Sensitive Data Leaked." New Delhi, August 27.

[43] UNIDIR. (2013). The Cyber Index: International Security Trends and Realities. New York and Geneva: United Nations Institute for Disarmament Research.

[44] Unnithan, S. (2012). "Enter the Cyber Dragon: India to Walk an Extra Mile to Match China's Achievement in Cyberspace." India Today, October 26.

[45] UNODA. (2011). Developments in the Field of Information and Telecommunications in the Context of International Security. New York: United Nations Office for Disarmament Affairs.

[46] Verma, A. K. and A. K. Sharma. (2014). "Cyber Security Issues and Recommendations." International Journal of Advanced Research in Computer Science and Software Engineering 4 (4): 629–634.

[47] Walstrom, M. (2016). "India's Electrical Smart Grid: Institutional and Regulatory Cybersecurity Challenges." Seattle: Henry M. Jackson School of International Studies.