THE NATIONAL CYBER SECURITY POLICY OF INDIA 2013: AN ANALYTICAL STUDY

Rajni Bagga[1]

I. Introduction

Rapid pace of innovation and increasing dependency on the internet has created an atmosphere of uncertainty and vulnerability making every country difficult to regulate the omnipresent cyberspace phenomenon. It has become impertinent for every country to address this issue with relatively comprehensive and bold security initiatives. Almost each country has issued its National Cyber security Strategy (NCSS) to strengthen cyber defence, cyber deterrence stance and build cyber capabilities.

The general definition of cyber security strategy/policy is a Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.[2]

"National Cyber Security Strategy (NCSS) is the nation's readiness strategy to provide cohesive measures and strategic actions towards assuring security and protection of the country's presence in cyberspace, safeguarding critical information infrastructure, building and nurturing trusted cyber-community".[3]

In simple words cyber security policy or strategy focuses on securing cyber space, securing e-governance services, combating cybercrime more effectively, revising the legal framework, promoting international cooperation and communication, raising awareness, and ensuring specialist

---

[1] Ph.D Reasearch Scholar, Dept. of Law, Punjab University, Chandigarh, email-baggarajni2011@gmail.com

[2] https://scottschober.com/glossary-of-cybersecurity-terms) Retrieved on 19 Dec, 2017.

[3] Oluwafemi Osho & Agada D Onoja, "National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis", 2015 International Journal of Cyber Criminology (IJCC) – Publisher & Editor-in-Chief – K. Jaishankar ISSN: 0973-5089 - January – June 2015. Vol. 9 (1) : 1 (http://www.cybercrimejournal.com/Osho&Onoja2015vol9issue1.pdf) Retrieved on 19 Dec, 2017.

education as well as the development of technical solution to counter attack the rising menace of cyber intrusions.

Few of the various objectives[4] while framing a cyber security policy are to develop and implement Legal & Policy Measures for combating cyber crime, regulate national cyber Incident response, Raise Public Awareness, strengthen cyber security Assurance Framework, Critical Information Infrastructure Protection, National Internet Safety measures, Promote Multi Stakeholder Partnership and Global Cooperation on Cybersecurity.

II. Why we need Cyber security policy/strategy?

National policies/strategies provide an important framework and roadmap for the security and growth of a country. Cyber space is a phenomenon which cannot be regulated through a single institution or agency. It requires a holistic and comprehensive approach and state sponsored mechanism in order to build a solid foundation for the establishment of cyber power and constructing more cyber-secure societies. It is true that cyber space is global challenge and difficult to control through domestic legislation but national policies provide important framework to promote international agreements and standards to support intergovernmental collaboration that put in place the educational and industrial policies.[5] National policies also provide necessary legal framework to regulate cyber crime and define the tools and mandates for security providers. Beside there are number of issues that can be taken care with elaborate cyber security strategies such as protection intellectual property rights, cyber espionage, cyber terrorism, innovation and patents etc.[6]

Following is the list of viable reasons to have a comprehensive cyber security strategy for each and every country in this digital era.

Economic growth of each and every country is dependent on the steady and secure Information communication technology infrastructure. Cyber security policy provides the required financial and technical capabilities for the economic growth of the state.

---

[4] Cyber Security Strategy" Estonia. (2014–2017) (https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf) Retrieved on 19 Dec, 2017.

[5] Dr. Detlev Gabel Bertrand Liard Daren Orzechowski, "Cyber risk: Why cyber security is important" published by White & Case LLP (2015) (https://www.whitecase.com/publications/insight/cyber-risk-why-cyber-security-important) Retrieved on 20 Dec, 2017.

[6] Narmeen Shafqat, Ashraf Masood, "Comparative Analysis of Various National Cyber Security Strategies", (IJCSIS) International Journal of Computer Science and Information Security, Vol.14, No. 1, January 2016.

Every state including India is now investing in the Information communication sector to digitize and accelerate the economic growth of the country. But at the same time increased dependence on the Information communication technology has also created vulnerabilities, risks and intrusions especially in critical infrastructure which is the backbone of every nation.[7] A comprehensive and holistic cyber security policy/strategy provide the security network while collaborating with the public-private sector raising the cyber defensive capabilities of the country.

As discussed earlier, there are number of emerging challenges such as legal complexities, jurisdictional issues, contractual issues, new cyber crime threats and risks making it difficult for any one organisation to deal with it effectively.[8] National Policy provides the solid foundations which regulate various agencies to work together and discharge the obligation entrusted upon them to make the cyberspace more secure and safe.

People are the most crucial link in securing cyber space. It is important that civil society made to understand the threat and impact of cyber attacks and make them prepared to tackle it before it can cause any danger. Malicious actors can affect the masses through cyber attacks, cyber frauds, and cause social upheaval through religious fanatics etc.[9] Respective government can regulate these outcomes by simply raising awareness among the masses about the harmful consequences of such acts as well as the protective means to be adopted while indulging in online activities. A comprehensive cyber security policy is an important tool that provides guidelines for the respective agencies to initiate campaigns to raise digital and informational literacy among all class of people whether old, young or housewives proving them with information to secure themselves in this digital world by encouraging individuals to take responsibility for their own online security. Only government has the required financial and administrative mechanism to help raise awareness in educational and other institutes against potential cyber attacks.

Each state can help build regional and international cooperation through elaborate cyber security policies and create the global cyber security culture. These policies are sign of commitment of a country towards cyber crime free society and encouraging International cooperation to deal with

---

7 ENISA. National Cyber Security Strategies - Setting the course for national efforts to streng then security in cyberspace. May 2012. Resilience and CIIP Program at ENISA. (resilience @enisa.europa.eu) Retrieved on 23 Dec, 2017.

8 Supra note 4

9 "Regulating Cyber-Security" Northwestern University Law Review, Vol. 107, No. 4, pp. 1503-1568, 2013; George Mason Law & Economics Research Paper No. 12-35. Available at SSRN: (https://ssrn.com/abstract=2035069) Retrieved on 25 Dec, 2017.

this menace. Many International agencies[10] such as UN, ITU and Organisation for Economic Cooperation and Development has been helping developing nations to raise the cyber security competence and capacity against cyber attacks.

A comprehensive cyber security policy is must for the comprehensive regulation of cyber space. It provides roadmap and focussed approach to regulate and control the negative effects of cyber space.[11] Cyber space influences the social, political, economical and personal aspects of our society today. It is impossible to live without information technology that is why it is considered the fourth revolution in the world and so far the most influential revolution of human life.

Various countries have enunciated the cyber security policies/ strategies to tackle the growing issues of cyber intrusions and its ill effects. We have already discussed the cyber security strategies of various counties in earlier chapters. In this chapter we will discuss and analyse the National cyber security policy of India released in 2013.[12]

III. Indian Scenario

Cyberspace has been evolving since its inception and at a rapid speed around the globe. Cyber warfare, cyber espionage and cyber terrorism are few of the most crucial aspect of cyber space that made all the countries suddenly worried about preserving their sovereignty at any cost. America is the first country that adopted and implemented the cyber security policy.[13] Later this trend was followed by various countries including United Kingdom, Australia and Japan etc. Cyber security is a term that cannot be taken lightly due to its various serious ramification impacting society, political framework and National security. There are few examples which made our lawmakers consider this aspect seriously and enact a security provisions for the same. At international level, the most serious example

---

[10] Panayotis A Yannakogeorgos, "Conflict and Cooperation in Cyberspace: The Challenge to National Security", dam B Lowther (Ed) CRC Press; 1 edition (2013)

[11] Atul M. Tonge, Suraj S. Kasture, Surbhi R Chaudhari, "Cyber security: challenges for society- literature review", Computer Law & Security Review Volume 29, Issue 3, June 2013, Pages 207-215 Computer Law & Security Review, 2013.

[12] Vipin Kumar, Jaideep Srivastava, Aleksandar Lazarevic "Managing Cyber Threats: Issues, Approaches, and Challenges (Massive Computing)", Springer; 2005 edition (2005)

[13] Department of Defense Strategy for Operating In Cyberspace. (http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf: US DoD. 2011). Retrieved on 26 Dec, 2017.

would be the cyber attack on Estonia in 2007[14] which literally paralysed the whole economy of the country including stock exchange, banking system and health care etc. At domestic level, in 2012, there was a circulation of information in Bangalore[15] targeting a community in a bid to disturb the communal harmony of the region. It was circulated to force that community leave the city within a stated date and also threatened of dire consequences if not complied with the demands. Offenders used social media and mobile phones to fulfil their evil plans and the impact was such that on 15 August 2012 there were hundreds of people who thronged the Bangalore railway stations in order to leave the city to avoid any mishap from the communal violence that might ensue.

Another example would be in May 2013, after the naxals attack in chattisgarh,[16] few anti national elements tried to misuse the power of cyber space by posting a page to explain full agenda of naxals, making them hero and demanded support from the people. Although government pulled off the page before it could do any harm but all these incidents definitely sent a warning to the government to regulate this issue as soon as possible. At Last 26/11 Mumbai attacks[17] were the last straw that forced the Indian government to come up with stringent cyber security strategy to combat this evil which has threatened the sovereignty of our country time and again. Government has realised the importance of cyber security framework due to rising cyber security challenges mounting day and night. Cyber security has become critical for the stable development of every nation today. Finally government of India released its First and much awaited National Cyber Security Policy in July, 2013.

IV. National Cyber Security Policy 2013

Digital revolution and increasing influence of information communication technology has affected every continent including ours. Same is the case with rising cyber threat since India is a developing country which makes us more vulnerable to the rest of the world in terms of cyber

---

[14] Babak Akhgar, Ben Brewster, "Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities (Advanced Sciences and Technologies for Security Applications)", Springer; 1st ed. (2016)

[15] Norma C. Noonan, Vidya Nadkarni, Palgrave Macmillan, "Challenge and Change: Global Threats and the State in Twenty-first Century International Politics", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 Volume 12, Issue 2 (May-Jun. 2013), PP 67-75 (*www.iosrjournals.org*) Retrieved on 26 Dec, 2017.

[16] Pavan Duggal, "Social Media and Mobile Law-Some Emerging Challenges", Saakshar law Publications (2015)

[17] Pavan Duggal, “Indian National cyber Security policy - A Legal Analysis” Saakshar Law Publications (15 January 2015)

security and defence. Cyber crime rate has been increasing at a massive rate in India.[18] To address this growing concern Indian government released its first National cyber security policy with an aim to monitor and protect information and strengthen defences from cyber attacks. The National Cyber Security Policy 2013[19] was released on July 2, 2013 by the Government of India. The purpose of this framework document is to ensure a secure and resilient cyberspace for citizens, businesses and the government. It was a much needed and much awaited step to regulate the rapid information flow and transactions occurring via cyberspace in India. Although it was a right step in the direction of establishing cyber security environment but it lacked various important component and elements to effectively deal with the multi facet issue called 'Cyber crime'.

The mission[20] of the policy is to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threat, reduce vulnerabilities and minimise damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

a. The objectives of the policy are:

(1) To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.

(2) To create an assurance framework for design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).

(3) To strengthen the Regulatory Framework for ensuring a Secure Cyberspace Ecosystem.

(4) To enhance and create National and Sectoral level 24×7 mechanism for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective response and recovery actions.

---

[18] Ravi Sharma, "Study of latest emerging trends on cyber security and its challenges to society", International Journal of Scientific & Engineering Research 3.6 (2012): 1.

[19] Pavan Duggal, "Indian National Cyber Security Policy- A Lagal Analysis". Saakshar Law Publications (2015)

[20] (*http://meity.gov.in/sites/upload_files/dit/files/National%20 Cyber%20Security%20Policy%20%281%29.pdf*) Retrieved on 27 Dec, 2017.

(5) To enhance the protection and resilience of Nation's Information infrastructure by operating a 24/7 national critical information infrastructure protection centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.

(6) To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition diffusion and commercialisation leading to widespread deployment of secure ICT products/ processes in general and specifically for addressing National security requirements.

(7) To improve visibility of integrity of ICT products and services by establishing infrastructure for testing & validation of security of such product.

(8) To create workforce for 5, 00,000 professionals skilled in next 5 years through capacity building skill development and training.

b. Strategies adopted by the Policy

- Creating a secure cyber ecosystem
- Creating an assurance framework
- Encouraging Open Standards
- Creating mechanisms for security threat early warning, vulnerability management and
- response to security threats
- Securing E-Governance services
- Protection and resilience of Critical Information Infrastructure
- Promotion of Research & Development in cyber security
- Reducing supply chain risks
- Human Resource Development
- Creating Cyber Security Awareness
- Developing effective Public Private Partnerships
- Information sharing and cooperation
- Prioritized approach for implementation
- Operationalisation of the Policy

The national cyber security policy is the first step taken by Indian government in regulating country's cyber security concerns. Government has included important guidelines or roadmaps that have to be taken by various cyber security stakeholders of the country. It is very good effort but

real challenge is implementation and realisation of the goals embodied in the document. Mere citing guidelines in a document will not be enough to control the ever growing issue of cyber security anywhere in the world.

c. Assessment of the policy

This policy being the first of its kind in India has both negative and positive points. First let us discuss the positive points of this policy in brief.

National cyber security policy of India has been released to cover variety of cyber security concerns in depth and holistic manner. It has many parts such as preamble, vision, mission, objectives and strategies to be adopted in order to regulate cyber space. Preamble of a document gives us useful insight into the minds of the policy/ legislation makers and the relevant purpose while drafting the document. It is thus an integral part of any legislation. The Policy starts with defining the term 'Cyberspace' in Para 1 as a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.[21] This throws light upon the growing impact and influence of information technology on our society as whole. In the next Para, importance and benefits of growing usage of cyberspace has been outlined with expectations of its future complexities to be on the rise due to mounting level of connectivity.[22] It has been highlighted how information technology has become one of the most significant growth catalysts for the Indian economy. This policy also highlight that secure computing environment and adequate trust and confidence in electronic transactions, software, services, devices and network is one of the compelling priorities while formulating the national policy. Preamble also explains the scope and impact of the cyber crime or attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures. It further clarifies that cyber related incident of national significance may take any form; an organized cyber attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets.[23] here the policy makers merged the national security threats and cyber crime incidents making these

---

[21] Supra Note 18.

[22] Nir Kshetri and Nir Kshetri, "Cyber security in India: Regulations, governance, institutional capacity and market mechanisms", Asian Research Policy 8.1 (2017): 64-76.

[23] Sanjiv Tomar, 'IDSA comment on National Cyber Security Policy 2013: An Assessment', (26 Aug 13) (http://www.idsa.in/idsacomments/ National Cyber Security Policy 2013_stomar_260813). Retrieved on 27 Dec, 2017.

two threats at par with each other while the fact is that security of national security infrastructure from cyber intrusion is far more important and fatal threat than cyber crime incidents such as online frauds or fishing etc. It also outlines few remedies to this growing menace like rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. In the last Para of the preamble, it was highlighted that the policy provides an overview of what it takes to effectively protect information, information systems & networks and also gives an insight into the Government's approach and strategy for protection of cyber space in the country. It also outlines some pointers to enable collaborative working of all key players in public & private to safeguard country's information and information systems.[24] This policy, therefore, aims to create a cyber security framework, which leads to specific actions and programmes to enhance the security posture of country's cyber space. In short preamble of the policy paints an appealing picture full of hopes and promises of bright future in order to have a secure and safe cyber security infrastructure in the country.

The vision of the policy is to build secure and resilient cyber space not only for the government but also for private entities and citizens which make this policy very ambitious. Mission of the policy also highlight the importance of coordinated efforts from people, institutions and advancement in technology for capacity building for preventing and responding to cyber threats, reducing vulnerabilities and minimizing damages in the wake of such attacks.

This policy has envisioned fourteen objectives to cover legislative, legal, technological, regulatory and social dimensions of this issue. Few of the impressive objectives are to enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, to operationalize a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC)[25] for security of the National Critical Information Infrastructure such as electricity, water and financial institutions etc., to create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training, to develop effective public private partnerships and to enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

---

[24] Report by Data Security Council of India, (Sep 13) 'Analysis of National Cyber Security Policy (NCSP – 2013)' available at URL: (https://www.dsci.in/sites/default/files/NCSP%202013_DSCI%20Analysis%20v 1.0. pdf) Retrieved on 27 Dec, 2017.

[25] "India's National Cyber Security Policy in Review" Jonathan Diamond. 31 July, 2013(.https://cis-india.org/internet-governance/blog/indias-national-cyber-security-policy-in-review) Retrieved on 27 Dec, 2017.

These objectives cover a wide range of topics, from institutional frameworks for emergency response to indigenous capacity building making it an aspiration document.[26]

There are number of strategies enlisted in the policy to achieve the goals/ objectives set out earlier. Some of the strategies adopted by the Policy include: Creating a secure cyber ecosystem through measures such as a national nodal agency, encouraging organisations to designate a member of senior management as the Chief Information Security Officer and develop information security policies, Creating an assurance framework, Encouraging open standards, Strengthening the regulatory framework coupled with periodic reviews, harmonization with international standards, and spreading awareness about the legal framework, Creating mechanisms for security threats and responses to the same through national systems and processes, National Computer Emergency Response Team (CERT-in) functions as the nodal agency for coordination of all cyber security efforts, emergency responses, and crisis management, Securing e-governance by implementing global best practices, and wider use of Public Key Infrastructure, Protection and resilience of critical information infrastructure with the National Critical, Information Infrastructure Protection Centre operating as the nodal agency, to promote cutting edge research and development of cyber security technology, human Resource Development through education and training programs to build capacity. The strategies outlined in the policy are very promising and holistic but lack depth as there are no roadmaps provided to implement the strategies.[27] Implementation of the policy/strategies is the most important aspect or responsibility of the government without which it is just a paper nothing else. This policy has prescribed various measures such as creating a secure ecosystem, creating a insurance framework, strengthening regulatory framework and securing e-governance services in order to protect and guard the critical information infrastructure. Other relevant strategy is to promote R&d in cyber security, promoting cyber security awareness and developing public-private partnership to foster sharing and cooperation among the various entities of cyberspace.[28]

This policy encourages adopting a focussed roadmap in order to designate a National nodal agency to coordinate matters related to cyber security in the country to be entrusted with responsibilities to tackle cyber threats of the future. To make the private sector responsible and prepared to

---

[26] Supra Note 18.

[27] Captain Sanjay Chhabra "India's national Cyber Security Policy (NCSP) and Organisation- A Critical Assessment". Naval War College Journal (2014). (https://www.indiannavy.nic.in/sites/default/themes/indiannavy/images/pdf/resources/article_6.pdf) Retrieved on 30 Dec, 2017.

[28] Supra Note 22

handle and mitigate cyber related incidents, this policy aims to encourage such sectors to establish a post of chief Information Security Officer (CISO) to regulate the cyber intrusions. The policy encourages such institutions to develop comprehensive cyber security policies at their respective institutions and implement these to increase the productivity of their businesses and promote customer's confidence. The said policy also encourages such institutions to allocate the budget for effective implementation of cyber security initiatives and to boost the capacity building efforts.

The said policy also encourages the stakeholders to create an assurance framework and adopting global best practices for enhancing the cyber security environment. It acknowledges the importance of complying with cyber security standards and guidelines such as ISO 270001 ISMS[29] certification etc. to create strong cyber security posture at domestic and international level. The policy further aims to have regular assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security.

V. Critical Analysis of the National Cyber Security Policy of India, 2013

Although the above stated policy has been appreciated and welcomed as the positive step towards cyber crime free society in India but still this policy overlooked and lacked various important issues concerning cyber space landscape. Some critic's[30] term this policy as too late and too little as far as practical aspect of the information technology infrastructure requires, whereas some are of the opinion that this policy is 'broad and lengthy' document with no depth what-so-ever.[31]

This policy is a welcome step which works as torch bearer to provide light and guidance to cyber security stakeholders present in public as well as private sector as to what steps these need to take collectively and individually to work towards safer cyber security ecosystem. It has also enlisted various strategies to be adopted to implement the projected vision of secure cyber ecosystem in the country. According to the cyber experts[32] this policy should have been released earlier since India has already has suffered from various cyber intrusion against national security servers and critical information infrastructure from neighbouring countries such as China and

---

[29] Jonathan Diamond, "India's National Cyber Security Policy in Review" 31 July, 2013.(https://cis-india.org/internet-governance/blog/indias-national-cyber-security-policy-in-review)

[30] Supra Note 18

[31] Supra Note 26

[32] Supra Note 23

Pakistan. The 26/11 attacks in Mumbai and Bangalore[33] cyber attacks caused a panic among the government prompting them to release the policy hurriedly. These attacks make the government realise that information technology cannot be taken lightly. Its effect and impact are far more serious and large scale than anyone could have imagined. Single breach in the critical information infrastructure can impact the whole country and create havoc within few seconds which is more dangerous than the physical attack by any country. Most of the countries have already released cyber security policies more than decade ago. Countries such as U.S and U.K are forefront in this regard.[34] These countries regularly review the work undertaken and initiatives completed under their country's cyber security policy and keep devising new action plans for the same. Whereas in India the policy enacted so late and without any Action plan to successfully implement the various objectives undertook in the policy.

Beside that there is another important pitfall that is lack of detailed instructions enabling relevant internet service providers to make them prepared in the wake of cyber attack to minimize the damage. There are no guidelines or roadmap provided in the policy to make the responsible stakeholder regarding potential cyber intrusion such as the cyber attack considering the fact that India has already been reported as the third most infected nation in the world.[35]

Another point of criticism is the absence of penal provision in the policy in case various stakeholders do no embrace the required cyber security mechanism in their respective institutions. These institutions are supposed to fulfil all the technological and computer network security requirements without any pursuance from the government. Private entities, most of who are in control of the critical information infrastructure in India should be held liable for any kind of breach that lead to financial and emotional damage to their customers.[36] Cyberspace has no borders which make it all the more dangerous for any specific country to regulate. Extra-territorial jurisdictional issues play an important part for the conviction of offenders belonging to different state. The National policy has completely overlooked this important issue. There are no guidelines or legal element

---

[33] Broadhurst, Roderic, and Lennon YC Chang, "Cybercrime in Asia: trends and challenges", Handbook of Asian criminology. Springer New York, 2013. 49-63

[34] "Global Cybersecurity Index. ITU. 2014. (http://www.itu.int/en/ITUD/ Cybersecurity /Documents /WP-GCI-101.pdf) Retrieved on 5 Jan, 2018.

[35] Strielkowski, Wadim, Inna Gryshova, and Svetlana Kalyugina, "Modern technologies in public administration management: a comparison of Estonia, India and United Kingdom." Administratie si Management Public 28 (2017): 174.

[36] Karnika seth, "Computer internet and New Technology Laws", Lexis nexis Publishing (2013)

stated to further the extra territorial jurisdictional issue which is the most complex issue so far.[37]

Individual privacy or freedom of speech which is an integral part of our constitution faces a huge threat in today's digital world. Government is responsible for the protection of the privacy rights of its citizen's as well as protecting the freedom of speech.[38] Balancing these rights is the most crucial issue. The present policy has completely failed to strike the balance between the privacy rights and national security issues. Beside the policy failed to prescribe various details and processes as to how the relevant stakeholders of critical infrastructure will protect the system when faced with any cyber intrusion. The policy has been drafted in an ambiguous manner without any detailed parameters for its successful implementation. Government has not put in place any mechanism to overlook the proper implementation of the stated policy and send regular reports regarding the same to the government. Cyber crime is increasing at a rapid pace in India due to the lethargic attitude of the government regarding regulating cyberspace with effective and holistic provisions. In the last few years India has witnessed a remarkable increase in cyber threats. As per the report of Indian Computer Emergency Response Team (CERT-In), a total number of 44,679, 49,455 and 50,362 cyber security incidents were observed during the year 2014, 2015 and 2016, respectively.[39] There is no sign of any significant decrease in such incidents till today, explaining the lack of required cyber security infrastructure in India.

Another important loophole is the lack of stringent legislative measures to regulate the cyber intrusion activities happening with mobile resources. Mobile users are increasing in India at a rapid speed with internet connectivity making it vulnerable to cyber attacks due to lesser security provisions embedded in those. India has already been reported as being the most vulnerable country from cyber attacks in the world.[40] To strengthen the security paradigm of our country there is need to establish an implementation mechanism, review cyber security legislation, raise awareness in the end-users as well as promoting global and domestic cooperation among various stakeholders to counter the rising cyber threat in India effectively. The most fatal threat today in front of various countries is cyber terrorism. Present policy does not provide any guidelines regarding the most evil threat of whole world. Although Information Technology Act

---

37 Amos N. Guiora, "Cybersecurity: Geopolitics, Law, and Policy", Routledge; 1 edition (2017).

38 "Supra Note 34

39 (//economictimes.indiatimes.com/articleshow/57051677.cms?utm_source= contentofinterest&utm_medium=text&utm_campaign=cppst) Retrieved on 7 Jan, 2018.

40 Ibid

2000 has been amended and Sec.66 F inserted via Amendment Act of 2008[41] to define and penalise cyber terrorism which does not cater to the required efforts to control and mitigate this growing menace. Single provision is not enough to deal with this huge security threat so there is an urgent need to have detailed legislative and regulatory framework with political, legal and technical infrastructure. The present policy completely overlooked this issue of immense importance of national security.

India is still awaiting the implementation of the cyber security policy which does not fully covers the basic cyber security requirements let alone the new and emerging issues such as cashless economy, e-governance, Adhaar, rising level of imported digital gazettes from China, Cloud computing and cyber radicalisation etc.[42] It does not provide binding guidelines to promote cooperation among various agencies responsible to counter cyber crime. It basically emphasise on the defensive capability of the country whereas it is time to focus on both defensive as well as offensive capacity building to tackle the new, improved, upgraded and sophisticated state sponsor cyber attacks. The policy does not mention about strengthening the offensive capability of the country.

According to PWC research report[43] there has been huge losses reported by private companies due to cyber breaches and losses per security incident which is a cause of concern. In spite of having cyber policy in place since 2013, there is no evident change or decrease in the cyber breach incidents rather it has been on the rise, increasing the sense of insecurity in the minds and lives of citizen or businessmen alike. The main reason for the growing cyber crime is ill preparedness and absence of stringent measures on part of the government in spite of experiencing many cyber security incidents such as 26/11 and Bangalore cyber intrusions etc.[44] Here the offender is far more advanced, highly skilled, fast, more aggressive in terms of technology and finance than the defender, making it more convenient for the culprit in pursuing their evil plans.

India is presently facing many types of cyber security threats. These include sophisticated cyber attacks, cracking, child pornography, cyber stalking, denial of service (DoS) attacks, distributed denial of service

---

41 Bamrara, Dr, Gajendra Singh, and Mamta Bhatt, "Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector." (2013).

42 Supra Note 21, Pg 64-76

43 "Pwc Global State of Information Security Survey 2015" (https://www.scribd .com/document/2590254 88 /Pwc-Gl obal-State-of-Information-Security-Survey-2015) Retrieved on 9 Jan, 2018.

44 "India's national Cyber Security Policy (NCSP) and Organisation- A Critical Assessment" Captain Sanjay Chhabra. Naval War College Journa (2014). (https://www.indiannavy.nic.in/sites/default/themes/indiannavy/images/pdf/resources/article_6.pdf) Retrieved on 9 Jan, 2018.

(DDoS) attack, malware infections, zero day vulnerabilities, phishing attacks, data theft, etc. In June 2012, cyber attacks were reported on the Indian Navy's Eastern Command systems.[45] On July 12, 2013,[46] just few days after the release of the National Cyber Security Policy, several high-level GOI officials reported their emails had been hacked. A report later on revealed that almost 12,000 systems were hacked which included systems from the Ministry of External Affairs, Defence Research and Development Organisation, Ministry of Home Affairs, National Informatics Centre etc. There are also few reports of Pakistan indulging in threatening cyber warfare. Hacker groups based out of Karachi and Lahore have in recent years managed to hack the websites of the Central Bureau of Investigation (CBI) and the Bharat Sanchar Nigam Limited (BSNL) mostly to leave hate mail.[47] It is widely believed that regional terrorist outfits, like the Indian Mujahideen (IM) have also made use of social media sites to communicate effectively. These are the few important initiatives discussed above but right now there is an urgent need to have a speedy and robust cyber security system in place to counter the growing cyber risks in India.

VI. Conclusion and Recommendations

To conclude it can be said that the present national cyber security policy unveiled in 2013 is highly defective and ill drafted to address the present security threats. Its various drawbacks have been discussed earlier which indicates that it is time to draft and implement new and revised policy keeping in mind the emerging threats and risks in cyberspace. Current cyber security requirements have completely changed due to the changing information technology posture considering the various projects launched by India government to digitally empower India and to lure the international companies invest in India. Digital India project, smart cities project, Adhaar card project and recently encouraged cash less India campaign add new dimension to the cyber security framework.[48] From organisational point of view, There are multiple agencies like Ministry of Electronics & Information Technology (MeITy), National Critical Infrastructure

---

[45] Rumani Saikia Phukan, "Encryption Policy and Cyber Security Problems in India" November 16, 2015 by (https://www.mapsofindia.com/my-india/government/encryption-policy-and-cyber-security-problems-in-india) Retrieved on 27 Jan, 2018.

[46] "Cyber Security Problems And Challenges in India" December 7, 2015 Report By Perry4Law Organisation (P4LO)http://cjnewsind.blogspot.in/2015/12/cyber-security-problems-and-challenges.html) Retrieved on 29 Jan, 2018.

[47] "Cyber Security Problems And Challenges in India" December 7, 2015 Report By Perry4Law Organisation (P4LO) http://cjnewsind.blogspot.in/2015/12/cyber-security-problems-and-challenges.html) Retrieved on 29 Jan, 2018.

[48] Pavan Duggal, "Indian National Cyber Security Policy- A Lagal Analysis", Saakshar Law Publications (2015)

Information Protection Centre (NCIIPC) under National Technical Research Organisation (NTRO) for safeguarding critical infrastructure and Indian Computer Emergency Response Team (CERT-In), which works under Meity but there is no one to monitor and operate all the cyber security activities undertaken by these agencies as there is no cooperation and information sharing mechanism in place. There is utter shortage of cyber security personnel in the CERT-in which creates a hurdle while handling the data security and breach incidents in a short time span. The government should focus on imparting training to more IT professional and there should be workshops at college and university level to train the young minds for their own security since young generation is more addicted to online activities. Second level of cyber security professionals that we need are the hands-on experts who are skilled in the five major functional areas of cyber security as defined by NIST (National Institute of Standards and Technology) – Identify, Protect, Detect, Respond and Recover. As estimated by NASSCOM's Cyber security Task Force[49], India needs 1 million trained cyber security professionals by 2025. The current estimated number in India is 62,000. Not only young people but police department and judiciary must also be provided with all necessary training regarding techno-legal issues to effectively deal with prosecution of cyber criminals. The government should also review and revise the IT act, 2000 to cover the latest cyber security issues such as digital payments and mobile banking which is the most complex and challenging issue today. In order to empower digital India projects, first we need to empower our cyber security infrastructure by drafting a holistic and comprehensive cyber security strategy with clear cut and detailed provisions to take care of the emerging cyber security risks. There is lack of detailed regulation of relationship regarding public-private partnership in case of critical sector infrastructure where most of the entities are private entities. Although government has established Sectoral CERTs but there are no guidelines regarding the liability for high impact cyber attacks on the most vulnerable critical information infrastructure.[50] Government must formulate a plan to encourage the public-private partnership through various fiscal benefits and incentives to motivate a robust cyber security practice among CII operators. Projects like Aadhar, National Intelligence Grid (NATGRID), Crime and Criminal Tracking Network and Systems (CCTNS), National Counter Terrorism Centre (NCTC), Central Monitoring System (CMS), Centre for Communication

---

[49] "Nasscom task force to make India hub for cyber security research' May 26, 2015, (//economictimes.indiatimes.com/articleshow/47421520.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst) Retrieved on 2 Feb, 2018.

[50] Jonathan Diamond, "India's National Cyber Security Policy in Review". 31 July, 2013 (.https://cis-india.org/internet-governance/blog/indias-national-cyber-security-policy-in-review) Retrieved on 2 Feb, 2018.

Security Research and Monitoring (CCSRM), Internet Spy System Network and Traffic Analysis System (NETRA) of India, etc are in violation of Civil Liberties Protection in Cyberspace.[51] None of them are governed by any Legal Framework and none of them are under Parliamentary Scrutiny. The proposed National Security Policy of India must address this issue as well on a priority basis. The privacy issue, ignored by the present cyber security policy must be immediately addressed by formulating a separate privacy legislation making it mandatory for service providers and law enforcement agencies to respect the personal space of an individual while protecting the national security infrastructure. Government should formulate the security keeping in mind the technological needs of the country not the political ones as we are living in digital age where everything from social to political is influenced by the cyber space. Some cyber security experts are of the view that Indian Government should establish National Cyber Security Agency (NCSA) to improve the cyber defence mechanism as well as cyber resilience of India.[52] Government should establish a check and balance mechanism to inspect the cyber security tools imported from other countries to look for hidden hacking tools, malware, trojans or tracking tools making our security system more vulnerable to cyber espionage or cyber warfare. With mobile cyber crime on the rise, it is time to conduct a mass awareness programs at schools, colleges or state level to educate people about different ways to protect them while using phones for online activities. Cyberspace cannot be monitored by the government alone, it is the collective responsibility of all stockholders to work together to form a robust cyber security mechanism to ward off the growing evil of cyber intrusions. Government should formulate a comprehensive strategy with detailed roadmaps and binding provisions for the preservation of cyberspace against any potential threat. India must learn from other Nations to draft, implement, evaluate and revise the Cyber security legislation with dedication and hard work. After all 'change' is the only thing which is static in cyberspace.

---

[51] Nir Kshetri, and Nir Kshetri, "Cybersecurity in India: Regulations, governance, institutional capacity and market mechanisms." Asian Research Policy 8.1 (2017): 64-76.

[52] Sanjiv Tomar, “National Cyber Security Policy 2013: An Assessment", August 26, 2013 (https://idsa.in/idsacomments/NationalCyberSecurityPolicy2013_stomar_260813) Retrieved on 2 Feb, 2018.