International Journal of Applied Social Science
Volume 6 (7), July (2019) : 1937-1943
Received : 18.05.2019; Revised : 04.06.2019; Accepted : 18.06.2019

RESEARCH ARTICLE
ISSN : 2394-1405

Cyber Security System and Policy of India: Challenges and Prospects

GITESH KUMAR
Ph.D. Research Scholar
Department of Politics and International Relations,
Central University of Jharkhand, Ranchi (Jharkhand) India

ABSTRACT

This paper presented the cyber security system and policy of India. Prime Minister of India, Narendra Modi has started the digital India campaign which is one of them initiative of Government of India, aimed at the digitally enabling Indian people through boosting connectivity, expanding access, provoking electronic delivery of government's scheme and planning to the common people. Therefore, it makes progress on the systematic programme for integrating the information and is the most important that benefiting each and every citizen through digital initiative. From this perspective, India can face various type of challenges such as data localization and cyber-attack. Therefore, Indian military forces are under process of establishing a cyber-command as a part of solidification the cyber security of defence system. There are creations of cyber command which will involve a parallel hierarchical structure as being one of the most central stakeholders. While the main objectives of this policy are to aims at protection privacy of the citizen. Though, after four years since the proclamation of the Cyber Security Policy, India's cyber landscape has witnessed in the growing platform digitization as part of the Government's Digital India because more sophisticated cyber threats, particularly the Wanna Crypt and Petyaransom ware attacks in 2017-18 that hit Indian networks this year. These radical changes require a revision and update to India's policy on Cyber Security. Certainly, cyber policy in Indian government has multiple stakeholders, ranging from the Ministry of Electronics & Information Technology, National Critical Infrastructure Information Protection Center, the Ministry of Home Affairs created National Cyber Coordination Centre for the counter the misunderstanding investigative authorities.

Key Words : Digital India, Cyber Security, Threat, Infrastructure, Hackers, Digital World

INTRODUCTION

Cyber threat from the professional criminals has been growing continue to become more sophisticated activities. The state sponsored computer hacker focus on economic and political espionage and on making provisions for digital disruption. Those are developing digital attack capabilities increasing and have been appearing as the threat in the front of government. There are various types of attacks which are carried out also becoming gradually multifaceted areas. Combined various activities with it, the numerous attacks that the digital infrastructure of countries which face on a daily basis from non-state actors. This forms a direct threat to the economic benefits and cyber security activities[1] . These developments call for an enlarged effort to support the cyber-security infrastructure with the public and private agency.

Cyber attackers are highly motivated, well-funded as well as technically advanced engagements. Their

1. Cyber Security in India: Opportunities for Dutch companies, available athttps://www.thehaguesecuritydelta.com/media/com_hsd/report/218/document/Cyber-Security-in India.pdf Accessed on 26 March 2019

How to cite this Article: Kumar, Gitesh (2019). Cyber Security System and Policy of India: Challenges and Prospects. *Internat. J. Appl. Soc. Sci.,* **6** (7) : 1937-1943.

attacks posture a threat to national level initiatives including Smart Cities, and digital public identity management and E-Governance. The military organisations and private businesses agency have process momentous volumes confidential the data and information. The potential damages can't only lead to monetary losses, but also put national security at risk if critical information infrastructure is targeted.

India is seen as a preferred out sourcing destination globally and key global brands such as Apple, Sapient, Citi Bank, Bank of America, HSBC, DSM and so on, have set their global delivery centres which shared services and support services in the country. At the same time, India has been currently rolling out the world's largest area the Information and Communication Technology programme known as the 'Digital India', which is dedicated on efficient service delivery, improving access, governance from education to health, and moving to India towards digital currency in the coming year. The Indian digital countryside has seen an incredible amount of transformation in a small duration of time, having grown considerably over a comparatively in the short period (Chitrey *et al.,* 2012).

The programmes that are being undertaking in India in the area of cyber space, both on public as well as private level are enormous to provide a lot of opportunities to Indian digital transformation period. This indication shows that India can best self-assured to capitalize on the economic as well as social opportunities of digitalisation in India with a secure path, to protect national interests of India in the digital domain[2] .

To build up Comprehensive Implementation:

NCE Policy 2013 took a welcome first step in outlining the basic principles and India can approach cyber security. Though, India needs an updated policy to move beyond simply a statement of principles and outline how to operationalize cyber security, from training cyber security personnel, to establishing public-private partnerships, and to facilitating civil-military collaboration. The National Cyber Security Policy in a broadly emphasized a vision for creating a workforce of 500,000 professionals skilled in the field of cyber security by capacity building, skill development as well as training in the year 2013. An updated outline of Cyber Security Policy should outline specific guidelines for the training and recruitment of such cyber specialists in a time-bound manner[3] .

Both sector of public and private partnerships are significant elements of India's cyber policy as well. There are engaging the development as an effective of public private partnerships and collaborative engagements in the cyber security. Therefore, it focused technical as well as operational relationship, there are various industry partners such as the National Association of Software and Services Companies (NASSCOM), Data Security Council of India (DSCI) and Information Systems Audit and Control Association (ISACA), have collaborated to address private sector and cyber security. Another part of priority for a new cyber security policy must be promotion the greater civil-military cooperation on the cyber security. A group of eighty leading defense, strategic and intelligence officials for cyber security standards in the country. There the need for more regular, more formalized interaction among the civilian as well as military branches of public sector. India needs the rapid transformation of the cyber landscape and a more comprehensive framework and updates its Cyber security policy for the operation of the objectives of policy 2013 (Thakker, 2017).

Creating a Secure Cyber Ecosystem:

1. To enable a National nodal agency to organize all matters related to cyber security in India, with clearly defined roles and responsibilities.
2. To support with the public and private to responsible for cyber security efforts and enterprises.
3. To promotion all organizations to develop information security policies accordingly integrated with their business plan and implement such policies as per international best practices.
4. To safeguard that all agency reserve a specific budget for implementing cyber security initiatives regarding emergency and cyber incidents.
5. To deliver fiscal schemes and incentives to boost

2. Cyber Security in India: Opportunities for Dutch companies, available athttps://www.thehaguesecuritydelta.com/media/com_hsd/report/218/document/Cyber-Security-in India.pdf Accessed on 26 March 2019

3. Thakker, Aman (2017). 'It's Time For India to Update Its Cybersecurity Policy' available at https://thediplomat.com/2017/10/its-time-for-india-to-update-its-cybersecurity-policy/ Accessed on 22 March 2019.

entities, strengthen and advancement information infrastructure with respect to the cyber security.
6. To avert occurrence and recurrence of cyber incidents by way of encouragements for the technology development, proactive actions, and cyber security compliance.
7. To establish a mechanism for sharing data and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.
8. To encourage entities to adopt guidelines for obtaining of trustworthy cyber security and provide for gaining of indigenously manufactured cyber security that has security implications (Ministry of Communication and Information Technology, 2012).

Securing E-Governance services:

1. To command implementation of global security best practices, business continuity management and cyber crisis organization plan for all e Governance initiatives,
2. To reduce the risk of distraction and improve the security posture.
3. To encourage wider usage of Public Key Infrastructure in the country for trusted communication as well as communications.
4. To engage information security professionals and organisations to assist e-Governance initiatives and ensure conformance to security best practices (Ministry Of Communication And Information Technology, 2012).

National Cyber Security Policy 2013: A Comprehensive Analysis:

Ministry of Communication and Information Technology of Government of India has released a National Cyber Security Policy in 2013. The main objectives are to secure data or information, sovereign data, personal information, sovereign data, financial and banking information, and so on. NCSP in the year 2013 as an affirmative step in the right direction which has to empower integration of new activities as well as programs under an umbrella a framework with a cohesive vision, a set of sustained with the coordinated strategies. A complete ecosystem through a virtue to secure computing environment can be created in India. It precedes into consideration various modern expansions that are taking place internationally in the field of cyber security. There are operating in cyber space disclosures entities including governments, businesses and individuals to gathering the data. Both the challenges and risks include coordination of energies in the country. The protection of critical information infrastructure, supply chain risks of ICT, legal framework capable of addressing technology's challenges, vigorous criteria implemented by regular audits, cyber threat intelligence gathering, crisis management, incident response and broadcasting, information sharing amongst public and private agency, availability of cyber security experts, cyber-crime investigations and so on. NCSP leads a holistic assessment of all these challenges as well as risks, and to a great extent regarding a comprehensive policy. Therefore, the challenge is in implementation of the policy for founding the objectives. The policy provides necessities for operationalization by detailed guidelines as well as plans of action at various levels (Analysis of National Cyber Security Policy-2013).

It is the most important that NCSP makes the market driven versus regulatory approach. This approach appears to convey the market and regulatory driven policy. For example, the policy also motivates towards organizations to designate or collaborate civil society, develop information security policies, adopt guidelines for obtaining of trustworthy the technology providing the fiscal schemes and incentives to encourage organizations for encouraging information infrastructure and cyber security.

Another area of the NCSP is indigenous development of cyber security products by cutting advantage Research and Development. The policy direction to work with the industry by joint Research and Development projects and setting up Centers of Excellence that is commendable. This objective is in line with the Triad Policies of the government on Electronics, IT and Telecommunications. In the Securing Our Cyber Frontiers report that it has been emphasized which India should be able to mitigate security risks arising from obtaining of ICT products, especially from foreign wholesalers, and however take complete benefits from the global supply chain which includes access to the world class products, services and expertise at competitive prices (Analysis of National Cyber Security Policy-2013)

The salient features of NCSP cover the following characteristics:

1. To secure as well as resilient cyber space for the citizens and businesses.

2. Empowering aimed at reducing national vulnerability to cyber-attacks, cyber crimes, and also focused minimizing response and recover time and effective cybercrime investigation.
3. To objective at the level of public and private partnership necessities, cyber security related technology, national alerts as well as to secure of critical information infrastructure, capacity building as well as encourage the information sharing and cooperation.
4. Focused the integration collaboration and coordination between the stake holder entities in India
5. To support and promote the strategies with the NCS policy's objectives.

Challenges:

1. To costs, create hurdles for businesses and may destabilize innovation without necessarily improving security; Impact of mandatory measures on sectors that are not mature in security implementations.
2. Internet information Supply Chain risks positioning of original products as more secure products.
3. Implications of mandating procurement of verified cyber security products without adequate testing facilities and delay in procurements.
4. India requires a comprehensive policy for countering threats and to play in the International arena (DSCI Analysis of the National Cyber Security Policy, 2013)
5. Lack of awareness
6. Lack of national level architecture for Cyber Security
7. Shortage of trained workforce
8. Lack of co-operation and coordination
9. Lack of uniformity in devices used for internet access

Opportunities:

1. Justification of government actions on the cyber security by better coordination among different government agencies.
2. Change in the ICT attaining processes of orgs esp. critical sectors and e-gov projects to focus on security of products; driving the suppliers to develop security in products; also increase in acceptability of tested products.
3. Enhanced cooperation amongst the government agency and industry on cyber security substances.
4. Enhanced partnership and information sharing on cyber security threats.
5. Need to enhance maturity of security practices as well as promotion of security function within the organizations especially in critical sectors and e-governance activities.
6. Growth in demand for security professionals including managers, implementers, , auditors, trainers.
7. Increased investments in security giving the boost to cyber security products and services market in India;
8. Providing momentous opportunities to security product and services companies besides auditing firms.
9. Impetus to the domestic security industry esp. the startups offering niche and innovative security products.
10. Better coordinated Research and Development through collaboration of government, industry and academia.
11. Sensitization of citizens, consumers and employees on cyber security threats and basic and best practices.
12. Supply of products and services
13. Cyber Forensics
14. Policy and Regulation
15. Developing new products through Research & Development collaborations
16. Capacity Building both at government and industry

Need a Cyber Security Policy:

Most countries around the world as well as India, the cyber security consequence is one of qualified disorder and a sense of insecurity arising out of the broken reports of cyber espionage, cyber terrorism, cyber warfare and cybercrime. Like the complication has resulted in a virtual paralysis and Artificial Intelligence. Legal prosecution instruments have not shifted as works fast enough to handle with growing cybercrime. In recently, cyber-attack in India indicates that a wide variety of offensive procedures are being considered through various agencies. The lack of a coherent cybersecurity policy

will seriously obstruct with India's national security and economic expansion. It is essential that more attention at the highest levels is paid to ensuring that cyber-related vulnerabilities that can influence on cyber security which are identified and removed the cybercrimes (Desai, 2012). Therefore, a coherent and wide spread cyber security policy will have several major elements, including accurate conceptualisation of cyberspace threats; building of robust cyberspace by a strong measure such as technical, legal, strengthening of PPPs, international cooperation, and diplomatic, creation of tolerable organisational structures.

India's approach to cyber security has sofar been ad hoc and fractional because lack of national level policy. A number of organizations have been created nevertheless, their precise roles have not been defined nor has synergy been created among them. It surpasses a vast domain, this falls within the charter of the NSCS. However, there appears to be no institutional structure for implementation of policies (Tomar, 2013). There has not been enough thinking on the consequences of cyber security and cyber warfare. For the time being, various countries are seriously engaged in countering to their cybersecurity doctrines and strategies issues. There are some counties here like US, France, China, Sweden, European Union, South Korea, Singapore and so on. They are more actively engaged in safeguarding a safe and secure cyber environment for their citizens (Desai, 2012).

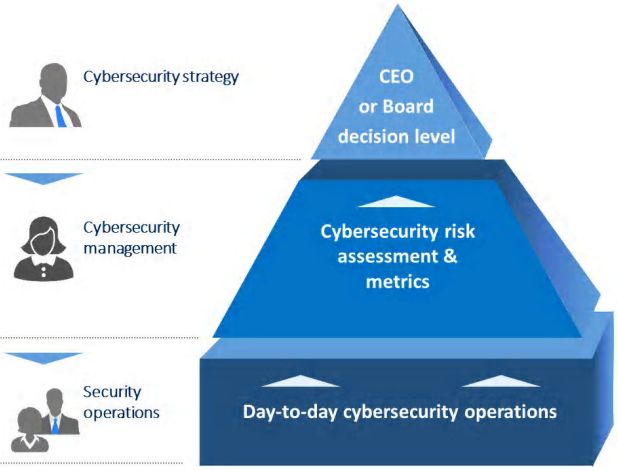
Cyber Security, Privacy and Freedom of Expression:

The paradox is that cyber security procedures anticipated to save the values of democracy which can end up actually eat away civil liberties such as individual privacy as the heart of the democratic setup. The balance between cyber security and freedom of expression needs to be smash into between national security and civil liberties. There are various government enterprises on cyber and national security including National Grid, designed as an NW of 21 available databases for both sector public and private agencies which meant to help counter possible terrorist threats and also the aadhar programme, which issued unique identity numbers, across the country (Desai, 2012). There have get up serious concerns towards privacy as the personal data are compiled in central databases and retrieved through the various government agencies. It is vital action and proper amendments the laws including a separate data protection and privacy legislation be put in place to protection against the misuse of such personal information as well as protect individual privacy.

Similarly, there prerequisite to the proper law amendments as well as procedural measures to ensure that the freedom of expression guaranteed under Article 19 of the Constitution of India.

Due to the unusual nature of cybercrime, existing methods approved through investigative agencies have been largely unsuccessful at the practical level. It becomes difficult to acquire evidence as well as perform investigative procedures (Tomar, 2013).

The identification of path of packets with the help of seizure the computers as well as storage media, collection of traffic data in real time, founding jurisdiction over practical offences and the power to collect data in real time which are some of the investigative methods that may be used by agencies. With regard to investigative measures, the cases that conveyed to light the need for the expansion of specific cybercrime investigative measures, the different procedures as well as techniques developed at the national and international levels that the provisions required by law agencies to work more efficiently and effective approach with general law and civil law countries. It needs to be considered upon to plug the existing ambiguities in the investigative methods



Source:https://www.google.com/search?safe=strict &hl=enIN &q=cyber+security&tbm=isch&tbs=simg:CAQSkwEJSNCm JNLRSRoahwELEKjU2AQaAAwLELCMpwgaYgpgCAMSKMADsROMCPEGvQHjCJMTsBOzE58Snj27KL49lTeTN8QuiiSN_1Q_1lD0aMPcwKLiNVESuBpodQlMe3 KulzlbPE4Dv5vnwgk Og8LkuaefCiX7xJDRFQO3zMP9zMCAEDAsQjq7CBoKCggIARIE3NHlCww&sa=X&ved=0ahUKEwisp7io8s3jAhU HmI8KHWrPCw4Qwg4ILigA&biw=1366&bih=657#imgrc=_ Accessed on 12 March 2019.

(Kedar, 2015). However, there can play a substantial role in weak cyber discouragement. The leading challenge that cyberspace in India faces is the multiplicity of cyber offences that have led to an urgent that need to place suitable tools for exploration as well as prosecution. There are major computer forensic centers like General Examiners of Questioned Documents at Chandigarh, Shimla, Kolkata, Hyderabad, and New Delhi. Furthermore, government set up the cybercrime centre for fighting infrastructure with effective manner.

International Status on Cyber security:

Cyber security is attractive an essential dimension of information security at the international platform. The rapid growth of computer system and Information and Communication Technology which has contributed enormously to human welfare but has also created risks in cyberspace, which can destabilise international as well as national security. The critical infrastructure is extremely susceptible to threats originating in cyberspace (Bamrara, 2013). Additionally, there are growth of social media including Twitter, Facebook, and so on that has created a new type of medium for strategic and policy in the communication, bypasses national boundaries and national authorities. The global data transmission infrastructure also depends critically on the NW of under sea cables, which is highly vulnerable to accidents and motivated disruptions (Desai, 2012).

The positive as well as negative potential of cyber security, there has been talk of formulating an international convention on cyber security which would safeguard that states behave responsibly in cyberspace. At the international level, already exist several international convention including biological toxins, chemical weapons convention, Non-Proliferation and weapons convention. Like this, time needs to counter of cyber-attacks. There is cyber warfare in three categories: 1. Espionage 2. Vandalism 3. Sabotage (Desai, 2012).

Conclusion:

It is fact that cyber criminals are highly educated which is a major challenge for the investigative agencies. This has enlarged the workload with the leading to an urgent action to considerably develop the number of the computer forensic laboratories in the country. Greater investment is required in the development of training centres for law enforcement officers and upgrading police stations so they can house the essential infrastructure to investigate cybercrime. Computer forensics must be the focal point for modernisation of the police. Moreover, the police must work closely with both governmental and non-governmental agencies, Interpol and the public at large, to develop a comprehensive strategy to address the problems.

Cyber threats can be disaggregated which is based on the offenders as well as their motives. There are four baskets namely, cyber espionage, cyber warfare, cyber terrorism, and cybercrime. Cyber attackers use several liabilities in cyberspace to constrain the mainstream work or action. They adventure the weaknesses in both software and hardware design by the use of international company. For instance, DOSS attacks are used to overpower the targeted websites and social media including Twitter, and Facebook account. Hacking activities is a common way of penetrating the defence of protected computer systems and the interfering with their functioning. So identity theft is also common in the mainstream.

REFERENCES

Badve, O., Gupta, B.B. and Gupta, S. (2016). Reviewing the security features in contemporary security policies and models for multiple platforms. In *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security* (pp. 479-504). IGI Global.

Bamrara, D., Singh, G. and Bhatt, M. (2013). Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector. *Gajendra and Bhatt, Mamta, Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector*.

Bamrara, D., Singh, G. and Bhatt, M. (2013). Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector. *Gajendra and Bhatt, Mamta, Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector (January 1, 2013)*.

Ben-David, Y., Hasan, S., Pal, J., Vallentin, M., Panjwani, S., Gutheim, P., ... and Brewer, E. A. (2011, June). Computing security in the developing world: A case for multidisciplinary research. In *Proceedings of the 5th ACM workshop on Networked systems for developing regions* (pp. 39-44). ACM.

Chaturvedi, M.M., Gupta, M.P. and Bhattacharya, J. (2008). Cyber Security Infrastructure in India: A Study. *Emerging Technologies in E-Government ', CSI Publication*.

Chitrey, A., Singh, D. and Singh, V. (2012). A comprehensive study of social engineering based attacks in india to

develop a conceptual model. *Internat. J. Information & Network Security*, **1**(2) : 45.

Data Security Council of India. 'Analysis of National Cyber Security Policy (NCSP – 2013)

Desai, Nitin (2012). 'India's Cyber Security Challenge' *Institute for Defence Studies and Analyses. Task Force Report.*

Halder, T. (2014). A cyber security for a smart grid. In *2014 6th IEEE Power India International Conference (PIICON)* (pp. 1-6). IEEE.

Kedar, M.S. (2015). Digital India: New way of Innovating India Digitally. *Internat. Res. J. Multidisciplinary Studies*, **1**(4) : 34-49.

Kumar, V. A., Pandey, K.K. and Punia, D.K. (2014). Cyber security threats in the power sector: Need for a domain specific regulatory framework in India. *Energy Policy*, **65** : 126-133.

National Cyber Security Policy, 2013 by Ministry Of Communication And Information Technology available at: https://nciipc.gov.in/documents/National_Cyber_Security_Policy-2013.pdf Accessed on 25 March 2019.

Santanam, R., Sethumadhavan, M. and Virendra, M. (2011). *Cyber security, cyber crime and cyber forensics: Applications and perspectives*. Information Science Reference.

Saraswat, V. K. Cyber Security Presentation [PowerPoint slides] (2018).

Shah, M. (2007). E-governance in India: Dream or reality. *Internat. J. Education & Development Using ICT*, **3**(2).

Ten, C.W., Liu, C.C. and Manimaran, G. (2008). Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Transactions on Power Systems*, **23**(4) : 1836-1846.

Thakker, Aman (2017). 'It's Time For India to Update Its Cybersecurity Policy' available at https://thediplomat.com/2017/10/its-time-for-india-to-update-its-cybersecurity-policy/ Accessed on 22 March 2019.

Tomar, Sanjiv. (2013). 'National Cyber Security Policy 2013: An Assessment' *Institute for Defence Studies and Analyses.* pp.1-7.

Ugale, B. A., Soni, P., Pema, T. and Patil, A. (2011, December). Role of cloud computing for smart grid of India and its cyber security. In *2011 Nirma University International Conference on Engineering* (pp. 1-5). IEEE.

Utreja, Savita. 'Cyber Security' Need for Proactive & Preventive actions' Ministry of Communications and Information Technology, Government of India.

****