Precise review of National Cyber Security Policy

Dr. Ramchandra Govind Pawar
Professor & Head Research,
Padmashree Dr. D.Y.Patil Institute of MCA, Akurdi, Pune – 44
Affiliated to Savitribai Phule University of Pune

1. ABSTRACT

National Cyber Security Policy has been implemented in 2013, here in this paper the researcher has taken the review of the policy how the policy is helpful to the citizens of India and the how the policy will help for the business and e-commerce. Until and unless the users are secure the people of the country will come forward for the use of the cyber space for the day to day activity as well as the business point of view. Where Cyberspace is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks. Having the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses, critical information infrastructure, military and governments in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace is expected to be more complex in the foreseeable future, with many fold increase in networks and devices connected to it.

Key words / Abbreviations: ICT – Information and Communication Technology, IT – Information Technology, PPP – Public Private Partnership, CISCO - Chief Information Security Officer, CERT-Computer Emergency Response Team, NCIIPC - National Critical Information Infrastructure Protection Centre, ICAN - Internet Co-operation for Assigned Names

2. INTRODUCTION

Information Technology (IT) is one of the critical sectors that rides on and resides in cyberspace. It has emerged as one of the most significant growth catalysts for the Indian economy. In addition to fuelling India’s economy, this sector is also positively influencing the lives of its people through direct and indirect contribution to the various socio-economic parameters such as employment, standard of living and diversity among others. The sector has played a significant role in transforming India’s image to that of a global player in providing world-class technology solutions and IT business services. In the light of the growth of IT sector in the country, ambitious plans for rapid social transformation & inclusive growth and India’s prominent role in the IT global market, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks, has become one of the compelling priorities for the country. Such a focus enables creation of a suitable cyber security eco-system in the country, in tune with globally networked environment. Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, can take place. Cyber 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. A 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. Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, supply chain attacks, data leakage, etc. There are various ongoing activities and programs of the Government to address the cyber security challenges which have significantly contributed to the creation of a platform that is now capable of supporting and sustaining the efforts in securing the cyber space. Due to the dynamic nature of cyberspace, there is now a need for these actions to be unified. The cyber security policy is an evolving task and it caters to the whole spectrum of ICT users and providers including home users and small, medium and large enterprises and Government & non-Government entities. It enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs. 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.

3. AIMS

The main aim of Cyber Security Policy is to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation. To enhance the protection and resilience of Nation’s critical information infrastructure by operating a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources. To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy. To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem. To enhance and create National level 24 x 7 mechanisms 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. To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people). To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention. To create a culture of cyber security and privacy enabling responsible user behavior & actions through an effective communication and promotion strategy. To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace. To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.

4. KNOWING ABOUT INDIA’S CYBER SECURITY POLICY
Following the rising number of cyber threats, the Indian government has gotten serious about securing the cyber space of the country. Earlier in 2013, the government had released the National Cyber Security Policy (NSCP) of India. Soon after that it released guidelines by the National Critical Information Infrastructure Protection Centre of the National Technical Research Organization (NTRO), the country’s elite technical intelligence agency. The Cyber Security Policy provides a strong vision to secure the critical infrastructure of the country. The policy was essential to prevent and reduce cyber attacks on public as well as private infrastructure. The policy also intends to circumvent any resultant economic instability arising due to cyber attacks. While the authorities agree that the real challenge lies in making this policy operational Things one should know about India’s National Cyber Security Policy 2013:

1. Set up a 24×7 National Critical Information Infrastructure Protection Centre (NCIIPC) for protecting critical infrastructure of the country.
2. Create a taskforce of 5,00,000 cyber security professionals in next five years.
3. Provide fiscal schemes and benefits to businesses for adoption of standard security practices.
4. Designate CERT- Computer Emergency Response Team as the national nodal agency to co-ordinate cyber security related matters and have the local (state) CERT bodies to co-ordinate at the respective levels.
5. All organizations to designate a CISO-Chief Information Security Office and allot a security budget.
7. Develop a dynamic legal framework to address cyber security challenges (Note: The National Cyber Security Policy 2013 does not have any mention of the IT Act 2000)
8. Encourage wider use of Public Key Infrastructure (PKI) for government services.
9. Engage IT professionals / organizations to assist e-Governance initiatives, establish Centers of Excellence, cyber security concept labs for awareness and skill development through PPP - a common theme across all initiatives mentioned in this policy.
10. Apart from the common theme of PPP across the cyber security initiatives, the policy frequently mentions of developing an infrastructure for evaluating and certifying trustworthy ICT security products.

5. CYBER SECURITY AN IMPORTANT ELEMENT OF FOREIGN POLICY: NEED OF HOUR

With Internet governance likely to see an increased role for governments in coming years and with cyber security becoming central to the prosperity of nations, cyber diplomacy has emerged as a key focus area of foreign policy around the globe, eminent speakers at an international cyber conference Cyber 360 degrees said here on Tuesday. The centrality of a cyber security pact in talks between US President Barack Obama and Chinese Xi Jinping this week and Indian Prime Minister Narendra Modi’s own dedication of a sizable chunk of his time in the US for interaction with Internet companies were cited as examples of the emergence of cyber diplomacy at the forefront of foreign policy issues at the conference.

“The internet governance model that has been in existence over the past few decades is showing signs of change. Because the Internet developed in the US, it is natural that US companies have monopoly over the technical architecture. Governments have until now had little role in the running of the internet. But with the Internet Co-operation for Assigned Names (ICAN) now undergoing transformation, there may be some broad basing of internet governance model,” India’s deputy national
security advisor Arvind Gupta said at the conference organized by the Synergia Foundation.

“During the last decade the internet has grown tremendously. Today over 3 billion people have access to internet. In the next 10 years the growth is likely to come from developing countries. The developing world will be a looking at a stake in the governance of the internet,” he said.

The interest shown by US companies in the Digital India initiative of the Indian government in the course of Prime Minister Narendra Modi’s visit to the US is an indicator of the importance of the Internet in the future scheme of things, the deputy NSA said. The emergence of cyber security as a key area of concern for countries means that it could be used for domination strategies, he said.

“We are seeing trends where trade may be used as an instrument of pressure on cyber diplomacy. The tendency to use export import regimes to restrict the flow of cyber security technologies and products is a concern. This is particularly a threat for emerging countries,” Gupta said.

“Cyber security has become an important element of foreign policy due to its relevance to national security, public safety and economic development. Developing international agreements on how states should behave in cyberspace and how to achieve a stable and open Internet will become increasingly important for India as well,” the deputy NSA pointed out.

“The challenge before the government is to ensure that the Internet infrastructure being put in place is stable and secure. For that the government will also have to be sensitive to not just the national security concern but also the needs and sensitivities of the business,” Gupta said.

He said India has initiated dialogues on cyber security with the US, UK, Germany, the EU, France, South Korea, Russia, Japan and Australia where views have been exchanged on national cyber security policies, sharing of critical information, capacity building research and development and other issues. “Cyber diplomacy is a growing area. It requires an intricate knowledge of technology, law, politics etc. The Indian government is focusing on this,” he said.

Former Swedish Prime Minister Carl Bildt pointed out that the importance of cyber security in foreign policy had been highlighted by the fact that cyber attacks were a central subject in talks during formal meetings between the US and Chinese presidents recently.

Former Indian National Security Advisor Shivashankar Menon said that cyber space had not disrupted the existing world order but had played a significant role in magnifying existing trends.

“It has become a fresh domain of contention between states. It is true of land, seas, skies and outer space all of which we have successfully militarized. Exactly the same thing is happening in cyber space. You see it when cyber attacks become one of the main subjects of a Xi-Obama summit and then you realize that cyber has come into its own,” Menon said.

This shows that the National Cyber Security Policy has to be taken in very serious way, if we want to prosper as a economic power in the world. Because now a day’s many transactions, business, commerce is preferred through the internet and if our Security policies are not up to the mark then it will affect badly on the performance of the nations even though we are having the capacity to do.

6. DEVELOPING EFFECTIVE PPP - PUBLIC PRIVATE PARTNERSHIP
To facilitate collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in particular for actions related to
cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices. To create models for collaborations and engagement with all relevant stakeholders. To create a think tank for cyber security policy inputs, discussion and deliberations.

7. MISSING POINTS
Some key points from the draft version missing in the final policy:

- Initiative to establish a countrywide secure intranet for connecting strategic installations with CERT for emergency response and coordination.
- The draft policy had objectively set out actions for ensuring security by Service Providers, Corporate and SOHO.

- Of the 12 stakeholders identified in the draft, only four are mentioned in the policy.

8. CONCLUSION

The above paper express that India has to take Cyber Security Policy seriously and the whatever the reports given by the experts that are mentioned above like NSA Arvind Gupta and Former NSA Shivshankar Menon as well as dialog with USA, UK, Japan and European Nations will have to apply wisely to strengthen the power of the Cyber Security. So that fear in the minds of the user will disappear and India will emerge the power in the World of e-commerce. Missing points which are mentioned above, needs to be considered once again.

REFERENCES
[12] Cyber security framework for Smart Cities to be out soon: NASSCOM
[13] Ten things you should know about India’s Cyber Security Policy
[15] Cyber security an important element of foreign policy: Deputy NSA Arvind Gupta

Website:
5. https://www.pwc.nl/en/assets/documents/pwc-industrie-4-0.pdf