SSPC MONOGRAPH SERIES No. 2

INDIA'S NATIONAL CYBER SECURITY POLICY: GAPS AND THE WAY FORWARD

SAURABH SINGH

Society for the Study of Peace and Conflict
https://www.sspconline.org/

SSPC MONOGRAPH SERIES

CONTACT: sspconline@gmail.com

Layout & Cover: ***Excel Solutions, Noida***

Cover Design: Saurabh Singh

REVIEW: ***SSPC Monograph series manuscripts undergo a rigorous review and editorial process by in-house and external subject matter experts and scholars.***

PUBLICATION DISCLAIMER: ***The views expressed in this Monograph are those of the author, who holds responsibility for the Content, Research, and Presentation of facts contained in this work.***

Published by Society for the Study of Peace and Conflict, Po-Bo: 10560, JNU Old Campus, New Delhi, 110067 (www.sspconline.org)

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

1. **C&IS Division** – Cyber & Information Security Division
2. **CCI** – Critical Infrastructure of India; Critical Information Infrastructure
3. **C-DAC** – Centre for Development of Advance Computing
4. **CERT-In** – Indian Computer Response Team
5. **CFSL** – Central Forensic Science Laboratory
6. **DAI** – Directorate of Air Intelligence
7. **DeitY** – Department of Electronics and Information Technology
8. **DGP** – Director General of Police
9. **DIA** – Defence Intelligence Agency
10. **DIARA** – Defence Information Assurance and Research Agency
11. **DMI** – Directorate of Military Intelligence
12. **DNI** – Directorate of Naval Intelligence
13. **DRDO** – Defence Research and Development Organization
14. **ERNET** – Education and Research Network
15. **FDI** – Foreign Direct Investment
16. **GoI** – Government of India
17. **IAMAI** – Internet and Mobile Association of India
18. **IB** – Intelligence Bureau
19. **ICT** – Information and Communication Technology
20. **IDSA** – Institute for Defence Studies & Analysis
21. **IISc** – Indian Institute of Science
22. **IIT** – Indian Institute of Technology
23. **ISP** – Internet Service Provider
24. **IT –** Information Technology
25. **ITA** – Information Technology Act
26. **ITAA** – Information Technology Amendment Act
27. **ITI** – Industrial Training Institute
28. **JIC** – Joint Intelligence Committee
29. **MEA** – Ministry of External Affairs
30. **MeitY** – Ministry of Electronics and Information Technology
31. **MHA** – Ministry of Home Affairs
32. **MNC** – Multi-national Corporation
33. **MoD** – Ministry of Defence
34. **NASSCOM -** National Association of Software and Services Companies
35. **NCCC** – National Cyber Coordination Centre
36. **NCIIPC** – National Critical Information Infrastructure Protection Centre
37. **NCSC** – National Cyber Security Centre
38. **NCSP** – National Cyber Security Policy
39. **NCST** – National Centre for Software Technology
40. **NCW** – No Contact War
41. **NIB** – National Information Board

42. **NIC** – National Informatics Centre
43. **NICNET** – National Informatics Centre Network
44. **NIST** – National Institute of Standards and Technology (U.S.)
45. **NIT** – National Institute of Technology
46. **NSA** – National Security Advisor; National Security Agency (U.S.)
47. **NSC** – National Security Council
48. **NSCS** – National Security Council Secretariat
49. **NTRO** – National Technical Research Organization
50. **PMO** – Prime Minister’s Office
51. **PPP** – Public Private Partnership
52. **R&AW** – Research & Analysis Wing
53. **R&D** – Research & Development
54. **STQC** – Standardisation Testing and Quality Certification
55. **UNCITRAL** – United Nations Commission on International Trade Law
56. **UNDP** – United Nations Development Program

ABSTRACT

Ever since the events of document leaks by NSA's whistle blower Edward Snowden, countries around the world have become conscious about their cyber security measures. The leaked reports worked as a wake-up call for India. India was the top most priority target by American spy agency NSA. It was time when India realized the great need of a Cyber Policy. In the year 2013, Ministry of Electronics and Information Technology (MeitY) drafted India's first National Cyber Security Policy (NCSP). The policy is framed with a coherent vision and a dynamic set of stratagems for execution. It is aimed at building a secure and resilient cyber space for its citizens, businesses and government. It is considered to be a dynamic step in building the foundation of new India. The newly formulated policy is a holistic approach towards securing Indian Cyberspace. But over the years, it does not seem to be effective enough to safeguard the Indian Cyberspace. The implementation of the policy is poorly executed. Since the time, the policy was made public. It had been in the limelight for criticism by various scholars and organizations. As complex it defines the cyberspace, it stands out to be of the similar nature. This monograph is aimed at understanding the NCSP and its implications. It identifies various shortcomings of the policy. It also analyses data related to cyber security incidents in India gathered from CERT-In Annual reports for the period of 11 years (2006-17). After the brief analysis of policy and data, the study made some valuable inputs in the form of recommendations for the revision of NCSP and strive towards building a secure cyberspace.

Keywords: NSA, NCSP, Cyber Policy, Cyberspace, India

Acknowledgements

Amongst the many who made this experience worth the hard work, I'm grateful to the people who guided me and helped me in formulating this research by addressing some of the severe and serious issues regarding the National Cyber Security Policy of India.

I would like to thank Dr Sampa Kundu, Asst. Prof. Symbiosis School of International Studies, for constantly guiding and motivating me throughout the work. She has been very understanding and cooperative. I thank her for all the comments, inputs and valuable insights provided by her for this research which further helped me in the process of improvising my work. She has been a perfect mentor and an encouraging guide throughout my endeavour.

I would also like to extend my gratitude to Amb. (Retd) Gautam Bambawale, Distinguished Professor, Symbiosis School of International Studies for his encouraging words and valuable suggestions which helped me in improvising my understanding of the issue and the quality of the work.

This publication would not have been possible without the support and assistance of Mr Animesh Roul, Executive Director, Society for the Study of Peace and Conflict (SSPC) and his team for providing me a suitable platform to exhibit my research and guiding me in this endeavour.

Last but not the least, I would like to thank my parents and also my colleague & friend Ms. Farida Chawala who have been a great source of motivation during the course of my work and will always be. It certainly would not have been possible without their blessings and support.

Chapter 1
Introduction

"Supreme excellence consists of breaking the enemy's resistance without fighting"

Sun Tzu, The Art of War, (Griffith 1963)

With the advancement in technology and increasing number of internet users, the world is becoming more and more revolutionized and innovative. It has altered the face of global economy and connected more people. We now live in a world with two dimensions. One is real and another is the virtual. Everything is online and connected over a series of networks and systems. It is one complicated structure holding the world together. The cyber world has not only fostered economic growth and new business opportunities, but has also become an engaging platform to learn and connect with each other. However, along with such opportunities have emerged major challenges facing the cyber world today.

India formulated its National Cyber Security Policy (NCSP) in 2013 with the vision to integrate and build a strong, resilient and secure cyberspace for its citizens, businesses and government. The Policy is driven by various objectives which helps boost Information and Technology (IT) sector in India. In recent years, there has been a significant amount of investment in the IT industry. Government projects like Make in India, Digital India are attracting heavy investments from across the globe. The Policy aides the goal of a Digitized India set by Prime Minister Narendra Modi. Effective e-governance is another objective which the Policy makes easier to achieve. It supports online businesses and encourages various stakeholders in creating a secure cyber ecosystem.

The number of internet users in India are increasing by the day. Every small village is now connected to the online space, which increases the chances of cyber-attacks. Such vast users of internet in a country with very little awareness about cyber ethics and cyber security creates vulnerabilities. With such humongous workforce (mainly unskilled and unemployed), there lies a great responsibility on India to prepare itself for any possible threat/attack from the cyber world. This Monograph tries to analyse and understand the NCSP, highlights some of its shortcomings and provides recommendations.

1.1 Cybersecurity: An Overview

Cyber security threats are a persistent problem which evolves from various sources and behaves in riotous manner as they employ themselves in series of disruptive actions targeting individuals, big business houses, government institutions and other digital infrastructure. The consequences of such malicious activities can have a significant impact on the national security, economic stability, public welfare and overall wellbeing. The origin of the attack and identity of the perpetrator can be difficult to determine. They tend to use hijacked networks of various system as substitutions which makes it difficult to identify the attacker/s. Such disruptive use of IT challenge the nuances of the practicality of the digital world.

1.2 What is Cyber Security?

Cyber security plays a vital role in safeguarding the data and information, including various other internet-based services. Cyber security can be simply defined as the protection of information from various malicious activities and defending devices through which information can be harnessed such as servers, computers, smartphones, mobile phones, tablets, other electronic devices and systems. (Kaspersky, 2019) The term cyber security is also known as Information Technology Security or Electronic Information Security.

Cyber Security pioneer Joseph Migga Kizza (Kizza, 2005) in one of his most acknowledged books “Guide to Computer Network Security (2005)” tried to connect cyber security in terms of three different components:

i. Confidentiality

This clause defends the system data and information from unauthorised revelation. These are generally preventive actions (technical or non-technical) proposed to safeguard computers, computer networks and systems (hardware and software) and the information stored within them from any threat directed to breach personal or national security.

ii. Integrity

The integrity clause defends the system data and information against malicious threats which may try to alter the information or may deceive it with false information.

iii. Nonrepudiation

This clause provides with the identification of the perpetrator with the help of digital signature. With the help of this service, the origin of the cyber-attack and the identity of the sender is easily traced with the help of algorithms and digital signature. A digital signature is a cryptographic mechanism that is the electronic equivalent of a written signature to authenticate a piece of data as to the identity of the sender.

1.3 Cyber Security: Where does it come from?

The origin of cyber security can be traced back to the late 1900s when internet became available for public usage. Apparently, the need for cyber security came from an incident which unknowingly created a virus. In 1970s, a researcher named Robert Thomas developed the very first computer virus. He realised that it was possible for him to move his computer program over a series of network leaving few trials of sign behind from wherever it moved. He named his program "Creeper". This happens to be the first cybercrime in the history of human civilization. Soon after this incident, an American computer programmer named Ray Tomlinson, who also happens to be the inventor of email service, was impressed from this idea of virus. He worked on similar algorithm with an intent to fix whatever the virus was disturbing. He was successful and named his program "Reaper" (Java Point, 2011). It became the world's first anti-virus computer software. Since then the internet has become all about viruses and anti-viruses.

The need of cyber security can also be identified from some movies. The 1983 classic “Wargames” is an example of growing concerns on the issue of cybercrimes and security (Raytheon, 2018). The movie portrays the notion that how hacking became a new fashion at that point of time and how a smart teenager unaware of internet ethics hacks into the military supercomputer and accidently causes a multi-national nuclear threat exercise.

Literature too has shown increasing concerns for cyber security. In 1986 (Howard, 2013), Marcus Hess, a German, hacked more than 400 computers of Pentagon officials with the motive to sell classified information to the Russian KGB. But an American astronomer Clifford Stoll prevented that and later wrote the book “The Cuckoo’s Egg” in 1989 which is his first-person narrative explaining the entire series of events. The real-life incident challenges the norms of the cyber security. It highlights how countries have managed to device techniques and plant moles into the intelligence organizations to secure classified information. Issues related to cybercrime picked up momentum from late 90s onwards.

1.4 Aspects of Cyber Security

There are various types of cyber security depending upon the type of malicious activities affecting the digital and physical infrastructure (Comodo, 2018). Some common types of cyber security are:

i. Network Security

This adopts preventive measures (physical or software) by safeguarding and protecting the network from any unauthorised access or intrusion. It encompasses the whole system from privately owned computer networks to the entire internet itself.

ii. Data Security

Data is the most important asset of the digital world. It can be defined as the practice of safeguarding and protecting vital data and information from various malicious activities by adopting preventive measures (physical or software). The data is often stored on one computer or over a series of computer systems. Antivirus software and firewall defenders are mostly used in the data protection and security.

iii. System Security

The objective of the system security is to protect data and information from theft or any other sort of damage. It not only protects information from any security breach but also defends the computer's operating system from any malicious worm or virus.

1.5 Cyber Threats: Invisible yet Lethal

At present, cyber threats stand as one of the significant challenges which government and individuals are facing. (Taylor, 2018) It is exclusive in nature if compared with unconventional methods of modern warfare because of following reasons:

i. Use of Hijacked Networks of System – the perpetrators make sure that their whereabouts are impossible to locate. For which, they tend to use hijacked networks of various system as substitutions which makes it really difficult to identify the attackers.

ii. Containment of Impact becomes difficult – if for once the cyber-attack is successfully launched, it becomes really difficult to contain it at a single place. Within a stipulated time period, it can spread across various networks and systems causing a lot of impairment and possibly incapacitating the digital infrastructure. Therefore, the impact of the same cannot be contained.

iii. Low investment, harmful consequences – one of the dangerous things about cyber-attacks is that it doesn't desire for investment in terms of state-of-the-art military equipment and technology. Any person with some adequate computer and programming skills and a dilapidated laptop or a ramshackle smartphone can cause large-scale chaos.

1.6 Types of Cyber Threats

Cyber threats can be broadly divided into four different categories depending on the motifs of the perpetrators (SecureWorks, 2017):

i. Cyber Espionage

Cyber Espionage is defined as the malicious practice of acquiring classified or covert information, including intellectual property rights without the permission of the information holder. The motive behind such an act can be of personal, economic, military, or political gain. The perpetrator uses various methods and techniques such as use of computer viruses to breach or hack into an individual computer or a network and steal sensitive information.

ii. Cyber Crime/ Attacks

Cyber-attack can be defined as any sort of malicious attempt to breach or hack into the computer or a network of any individual or organization with an intention to harm, damage or destroy it. A cyber-attack usually has two set objectives – first, to disable or destroy the set target facility or digital infrastructure and second, to access the classified information stored on the network or a computer. A cyber-attack can be categorized as a Cyber-campaign, Cyber-warfare or Cyber-terrorism considering the intensity, level and nature of the attack. In order to commit a cyber-crime, a perpetrator searches for vulnerabilities within a computer or a network. These vulnerabilities can be in terms of software or hardware malfunction. A perpetrator employs various methods and techniques in order to exploit these weaknesses.

iii. Cyber Terrorism

Any act of terrorism directed towards the malfunction or destruction of cyber space with the help of digital technologies is known as Cyber terrorism. It can also be defined as the consolidation of cyber space and terrorism. It is mostly understood as nasty illegitimate attacks and threats of attacks against computers, networks, and information; when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Use of cyberspace by terrorist outfits or any illegitimate organization to plan a terrorist attack, recruiting people on the pretext of false ideologies, spreading false propaganda and malicious context in order to brainwash people, acquiring funding from online sources, and pursing illegitimate political or economic goals is considered as an act of Cyber terrorism.

iv. Cyber Warfare

The evolution of cyberspace has changed the face of the modern warfare method and techniques. Cyberwarfare is now considered as the fifth domain of war. Cyberwarfare can be defined as the use of malicious computer programme, virus or worm by a nation-state with an intention to cripple, harm, damage and destroy the digital infrastructure of another nation-state leading to severe consequences such as loss of life and property, economic instability, damage to various military installations, disrupting technologies and breach in national security.

Chapter 2
Research Design and Literature Review

A. Research Design

2.1 Research Objectives

i. The main objective of this Monograph is to understand and analyse the National Cyber Security Policy 2013.
ii. To discover shortcomings and loopholes in the cyber policy.
iii. To recommend some concrete and strategic steps which might be helpful in making India a cyber mature and cyber secure nation.

2.2 Hypothesis

India's National Cyber Security Policy (NCSP) 2013 is framed with a coherent vision and a dynamic set of stratagems for execution; however, on exposing it to the Indian cyber domain, the Policy is believed to have set high standards of goals and objectives which results into several shortcomings in addressing the vulnerabilities of India's Cyberspace.

2.3 Research Questions

1. NCSP-13 talks about creating a cyber workforce of 500,000 professionals but it does not define or discuss what kind of role these professionals will play in the broader picture. The question remains does India have adequate skilled workforce to drive the cyber security measures? How can India bridge the gap between policy recommendations and skill development?
2. NCSP-13 is silent about the role of many government organizations which look after the cyber activities. In such a situation, the question prevails, whether the present Indian cyber security ecosystem or cyber organizational structure is effective enough to tackle/handle any major cyber-attack/threat or security breach? Or does it require a new makeover?
3. Despite setting high goals and standards for building a secure and resilient Indian cyberspace, many terms and statements in the NCSP-13 lack transparency. Does this lack of transparency make the policy ambiguous in nature?
4. NCSP-13 does not acknowledge or mention the IT Act 2000. In case of conflict which of the two will have the greater significance?

2.4 Research Methodology

This Monograph has used empirical research method. The study used qualitative research methods in the form of secondary data analysis which consists of published papers, peer reviewed papers, books, journals, official government reports, news reports and other secondary sources. The study is built upon a thorough analysis of various researches and reports conducted over the last few years in the form of literature review which highlights and categories various aspects of cyber security. The study used quantitative research methods in the form of data collected from last 11 years CERT-In reports (2006-2017).

2.5 Research Limitations

The limitations of the research mainly lie within the constraints of unavailability of primary qualitative data and information collected by the researcher as first hand.

B. Review of Literature

Cybersecurity is an essential matter of national security. Therefore, it makes it's essential to have a well drafted and strictly implemented Cyber policy. Not only this, the policy must be well drafted and in co-relation with the national and economic policy. The aim of this review of literature is to understand and analyse the kind of research and analysis that has been done so far with respect to Cyber Security. This chapter also tries to highlight and understand numerous arguments, conclusions and recommendations by scholars, academia, armed forces personnel, and cyber security experts.

a. Cyber Security in India: Need of the hour?

"A Literature Review on Cyber Security in Indian Context" (Ghate & Aggarwal, 2017) is a paper authored by Shweta Ghate and Pragyesh Kumar for spreading knowledge regarding the issues related to cyber security and cyber-crime in India. It focuses on importance of being acquainted with the effects of cyber-crime with respect to recent activities and recommend solutions or methods to protect the individual/organizations from any type of malicious cyber activity. It also portrays the current state of cyber-crimes and cyber security in India and its consequences and implications.

The paper authored by Rajiv Kumar Singh (Singh R. K., 2015) addresses the increasing security concerns and implications of any form of cyber-attack or threat in India. It focuses on the key amendments made in the 2008 Act which have brought many noteworthy changes in the IT Act, 2000, though there are many things still left to address. The paper challenges the dynamics of the policy making with respect to the cyber domain. The paper supports the nuances of effective e-governance, e-commerce and e-communications.

b. Cyberterrorism: A Primary Concern?

Authors Binny Pal Singh and Ankit Verma in their paper titled "Cyber Terrorism – An International Phenomena and an Eminent Threat" (Singh & Verma, 2015) talk about e various motifs and goals of terrorist organizations behind any cyber-attack. They try to understand how terrorist make use of internet for campaigning, advertising and recruiting.

The paper titled as "Future Towards Danger: The Terror of Cyber Attacks" (Sharma & Bhalla, 2015) explores various definitions of cyber terrorism and discuss various forms of cyber-attacks. The paper analyses some of the major risk involved in the act of cyber terrorism and reconnoitres some preventive measures.

"A Biggest Threat to India – Cyber Terrorism and Crime" is a paper (Naik, 2017) which talks about some definitions related to cyber terrorism and cyber-crime. It also focuses on the method and tools of attacks that are employed for prosecution of cyber-attack. The paper explores various arguments that explains how India's national security is affected from such cyber-attacks and activities related to cyber terrorism.

The paper titled "A Critical Study on Cyber Terrorism with Reference with 26/11 Mumbai Attack" (Hani & Rajan, 2018) analyses the term "Cyberterrorism" and tries to define the same in context of the 26/11 Mumbai attacks. It talks about the various challenges that are being faced in countering cyberterrorism in India. The paper refers to many case studies relating to cyber terrorism and tries to examine it from the perspective of cyber laws.

c. International Cooperation: Securing Cyberspace or Neutralizing Cyberwarfare?

'A Study on Cyber Security, Its Issues and Cyber Crime Rates in India' (Mishra, Dhir, & Hooda, 2016) focuses on the global cyber security scenario and how the domain of cyberspace demands international cooperation. It also talks about the issue of cyber security as a whole and its practices. The paper conducted an analysis of the average crime rates in India within a stipulated time period of 4 years (2009-

13). The paper also discusses in brief the counter measures that have been adopted by the government.

Another paper titled Cyber Security in India: Problems and Prospects (Devi & Rather, 2015) addresses various concerns from the increasing technological advancement in IT. The paper highlights that the inter-state relations have drowned into securing their economic stability and maintaining national security and have certainly forgotten about the severe implications from the cyber world. The paper also stresses upon the fact that since there exists no balance of power in the cyber world, cyber-attacks seem to have enough potential to convert the security dilemma of states into real acts of aggression. Therefore, such an understanding of events demands a strong international cooperation.

"Cybercrime and Information Warfare – The New Arena of War" (Pathak & Sharma, 2015) stresses upon the severity of newly defined and acknowledged warfare – 'Information Warfare'. Such warfare takes place when one nation seeks to sabotage the digital infrastructure (encompassing of information systems) of another by disrupting, damaging or harming it. The paper tries to give a brief understanding of such kind of warfare which is often acknowledged as No Contact Warfare (NCW). The paper talks about the preventive measures to be taken in order to prevent cyber-crime.

The book titled "Securing Cyberspace: International and Asian perspectives" (Samuel & Sharma, 2016) talks about the Cybersecurity issues with respect to the Asian perspective. The book is divided into two sections: International perspective on cybersecurity and Asian perspective on Cybersecurity mainly focusing on the various facets of securing cyber space with respect to the increasing amount of data flow towards the South and South East Asia.

d. Establishing a Nexus and Initiating a Dialogue: Public Private Partnership (PPP)

The Task Force Report published by IDSA (Institute of Defence Studies and Analysis) titled "India's Cyber Security Challenges" (Desai, et al., 2012) is a masterpiece on cyber security challenges faced by India. It helps in defining cyber security by providing an overview. It talks about cyber war and why a country like India should be prepared for it. It also sheds some light on the new public-private partnership (PPP) patterns and how it is responsible for protection of critical information infrastructure. It also highlights the importance of bringing out a synergy between the national policy and the international cooperation.

"Pyramid: A case study of Cyber Security in India" (Singh & Rishi, 2015) presents a case study on a company called *Pyramid Cyber Security (P) Ltd.* which specializes in the field of cyber security. The authors look into the matters of digital crime, fraud and forensic solutions and services in India. The paper portrays how private entities are the key stakeholders in the cyber domain, especially when it comes to cyber security solutions. The paper talks about how cloud computing give companies easy access to product and services and also the ease of doing business. But with increased opportunities, there comes the grave danger of cyber threat and cyber-attack to businesses. Such a scenario has placed these cyber security companies in a state of dilemma – whether to focus on existing business or explore new opportunities.

The paper "Cyber Security in India: Present Status" (Mallick, 2017) draws a comparison between the United States Cyber Security Policy and Architecture and Indian Cyber Security Policy and Architecture and brings out the differences between the two. It highlights the fact that India is trying to analyse the U.S. cyber security policy and produce a strategic document in context with its national security. The issue brief is directed towards the security community of India and various other cyber experts, academia and private entities looking after the cyber security nexus by providing cyber security solutions to various economic stakeholders.

The paper titled "Cyber Security Issues and Recommendations" (Verma & Sharma, 2014) focuses on the need for various stakeholders such as academia, business houses, think tanks, government organizations to come together and discuss issues related to cyber security. Lack of dialogue between various stakeholders makes it difficult to form a profound and strategic policy in sync with the national security. The authors acknowledge that the need of cyberspace and its exploitation is growing rapidly. Hence, there is a significant need for international cooperation in fighting cyber-crimes.

e. Imparting Wisdom: Cyber Security in Education

The paper "Cyber Security: Challenges for society – Literature Review" (Tonje, Kasture, & Chaudhari, 2013) stresses upon the need to inculcate the habit of cyber-ethics, cyber safety and cyber-security among citizens and that too from a very tender age. Therefore, such issues need to be integrated in the educational curriculum. The authors highlight some of the new emerging trends in the field of cyber security and also show how it is adapting to new methods and technologies.

The main arguments of the paper are how there is a lack of so called 'nexus' between the security agencies and critical infrastructure.

"A Review of Indian Approach towards Cybersecurity" (Singh, Gupta, & Kumar, 2016) brings out the fact that though there might be a strategic policy in place to defend our cyberspace and fight cyber-attacks and cyber-crime but still there is a lack of general awareness among the people regarding the malicious activities related to cyberspace. The authors also focus on the fact that there is a considerable amount of gap between the policy making and implementation. The authors highlight the need to blend eastern and western ideologies to have a pro-active approach towards cyber security.

From the reviewed literature it can be deduced that majority of the papers and journals are talking about cyber security as a whole. Most papers are informative. The literature reviewed lacks the benefits of a concrete research question. Most papers do not have research questions. The research is quite subjective in nature. The research conducted in the reviewed literature is time sensitive, which means that results and conclusions deduced from such a research is out of context in the current scenario.

Chapter 3
Indian Cyberspace

3.1 Introduction

The Indian cyberspace can be defined as a complex environment consisting of interactions between computers, networks, servers and people supported by advancing information technology (MeitY, NCSP, 2013). There are many organizations looking into the matters related to cyber security in India. It's certainly difficult to trace the historical background of the Indian cyberspace since there are no official documents, papers or books which talk about it in detail.

3.2 National Informatics Centre (NIC)

The history of Indian Cyberspace can be traced back to the year 1976 when the NIC was set up. The sole objective of NIC was to provide IT solutions to the government. It was established under the aegis of MeitY's Department of Electronics & Information Technology (DeitY). The primary role of NIC is to steer e-governance application launched by Government of India at national, state and district levels. Majority of the government websites are developed and launched by NIC. In short, NIC provides all telecommunications and networking solutions to the government at various levels. It is regarded as the backbone of the telecommunication sector in India.

3.3 Important Networks of India in early 90s

During the 1980s, three most crucial networks were set up by MeitY.

i. NICNET (National Informatics Centre Network)

In order to provide internet services to government and administrative bodies throughout the country, NIC set up a satellite-based communication network which was named NICNET (m@dhu, 2012). It is the world's largest satellite-based communication network system. It provides IT solutions and enables exchange of information between various government bodies and other corporate and business houses. This network is best suited at times of disaster and natural calamities.

ii. INDONET

This network was set up in the year 1986. INDONET is regarded as the first commercial internet service provider (ISP) of the country. It provided IT services and solutions to individual users and corporate and business organizations. It inculcated the so called "network culture" in the country.

iii. ERNET (Education and Research Network)

This is an education and research-based project in joint collaboration between Government of India (GoI) and United Nations Development Program (UNDP) (m@dhu, 2012). The project was initiated with the objective to develop and inculcate a culture of Research and Development (R&D) in the country in the area of networking and internet. India's top eight finest technical institutions, including National Centre for Software Technology (NCST), Indian Institute of Science (IISc) and five Indian Institute of Technology (IITs) were part of the project. ERNET now has many collaborations with other educational institutions.

3.4 Indian Computer Emergency Response Team (CERT-In)

CERT-In is a national nodal agency set up under the aegis of MeitY. It deals with cyber security activities like hacking and phishing. The agency has been operational since 2004. It started bringing out comprehensive annual reports from 2006 that consist of all major and minor activities that affect any Indian organization or company. It collects data and performs a synthesis analysis of all the cyber incidents. It also forecasts alerts and issues advisories to various organizations. It trains IT professionals and other officials to deal with any sort of malicious cyber activities.

3.5 National Information Board (NIB)

NIB is India's top policy-making apex body on cyber security. The agency works under the direct supervision of Prime Minister's Office (PMO) and is headed by the National Security Advisor (NSA). Any policy matter related to cyber security are discussed in the board and upon further approval are passed on to National Security Council (NSC). NIB consists of 21 members, all of whom are secretaries to Government of India (GOI) (Singh V. , 2013).

3.6 National Cyber Coordination Centre (NCCC)

NCCC is an operational body that looks into the matter of cyber security and e-surveillance in India. It works in close coordination with other intelligence agencies on the issues concerning cyber security. It came into existence in 2014 and works under NIB. NCCC has been classified as a government cyber security project without any legal framework.

3.7 National Technical Research Organization (NTRO)

NTRO is the technical intelligence agency of India. It is solely dedicated to gathering technical intelligence. It has been operational since 2004 and works under the direct supervision of NSA in the PMO. The agency deals in developing state of the art modern technologies which helps in data gathering, remote sensing, cyber security and cyber forensics.

3.8 National Critical Information Infrastructure Protection Centre (NCIIPC)

NCIIPC is formed under Section 70A of the ITAA as a government organization. (NCIIPC, 2017) It is operational since the year 2004. It is designated as a national nodal agency for protection of critical information infrastructure. It has identified 'Power & Energy', 'Telecom', 'Banking, Financial Services', 'Transport', 'Strategic and Public Enterprises', and 'government' as critical sectors or critical infrastructure of India (CII). It acts to coordinate, share, monitor, collect, analyze and forecast national level threats to CII for policy guidance, expertise sharing and situational awareness for early warning or alerts.

3.9 Information Technology Act 2000 (ITA)

IT Act or ITA of 2000 is a law that deals with cybercrimes and digital fraud in India. The Information Technology Bill became a law on June 9, 2000. The 1996 United Nations Commission on International Trade Law (UNCITRAL) for adoption of model law on electronic commerce (e-commerce) became the basis of IT Act. The law is applicable in matters of e-commerce, digital fraud and cybercrimes. The ITA is divided into 19 chapters, 4 schedules and 94 sections. The Act classified cybercrimes against three categories:

i. Individuals;
ii. Society;
iii. Organizations;

The Act also amended various sections of Indian Penal Code 1860, India Evidence Act 1872, Bankers Book Evidence Code 1891, and Reserve Bank of India Act 1934 (MeitY, IT Act, 2000). Some of the major provisions under the IT Act 2000 are listed below in the table.

3.10 Information Technology Amendment Act 2008 (ITAA)

The ITAA is an addition to the IT Act of 2000 which became operational from October 27, 2009 (MeitY, IT (Amendment) Act, 2008). The additions were made in order to enhance the ITA. The amendment introduced Section 66A - publishing of false information which accounts to 3 years imprisonment, fine or both. The ITAA focused on data privacy, information security, introducing a new definition of intermediary, defining and acknowledging the role of CERT-In, acknowledging severe crimes like child pornography and cyberterrorism.

Table 3.9: Major Provisions Under Information and Technology Act 2000. (Source: MeitY)

Major Provisions under Information and Technology Act 2000				
Offence	**Computer as a Target**	**Computer as a Weapon**	**IT Act 2000 Section**	**Fine/ Penalty**
Physical Attack	✓		Section 43	Up to ₹ 1 crore
Virus	✓		Section 43	Up to ₹ 1 crore
Trojan Horse	✓		Section 43	Up to ₹ 1 crore
Forgery or Tampering documents		✓	Section 65	Up to ₹ 2 lakhs or imprisonment up to 3 years or both
Hacking	✓		Section 66	Up to ₹ 5 crore or imprisonment up to 3 years or both
Denial of Service (DoS)	✓		Section 66	Up to ₹ 1 crore
Data Manipulation		✓	Section 66	Up to ₹ 5 lakhs or imprisonment up to 3 years or both
Email related crimes		✓	Section 66A	Up to ₹ 1 crore
Receiving stolen computer or communication device		✓	Section 66B	Up to ₹ 1 lakh or imprisonment up to 3 years or both
Identity Theft		✓	Section 66C	Up to ₹ 1 lakh or imprisonment up to 3 years or both
Cheating using Computer resources		✓	Section 66D	Up to ₹ 1 lakh or imprisonment up to 3 years or both
Publishing private images of others without consent		✓	Section 66E	Up to ₹ 2 lakhs or imprisonment up to 3 years or both
Acts of Cyberterrorism		✓	Section 66F	Life term Imprisonment
Defamation		✓	Section 67	Up to ₹ 10 lakhs or imprisonment up to 5 years or both
Publishing Pornography and Child Pornography		✓	Section 67A & 67B	Up to ₹ 10 lakhs or imprisonment up to 7 years or both
Breach in Privacy		✓	Section 70 & 72	Up to ₹ 5 lakhs or imprisonment up to 10 years or both
Breach of Confidentiality		✓	Section 72	Up to ₹ 1 lakh or imprisonment up to 2 years or both

Chapter 4
National Cyber Security Policy (NCSP) 2013

4.1 Introduction

National Cyber Security Policy 2013 is an official document published by MeitY, that includes the roadmap of cyber security and framing a secure cyber ecosystem throughout the country. It is a 15-page document, including a preamble and five main focus points consisting of Vision, Mission, Objectives, Strategies and Operationalization of the Policy.

4.2 Background

The NCSP was initiated when 'The Hindu' (Greenwald & Saxena, 2016) in one of its reports revealed that India was the top target of snooping by the U.S.'s NSA. The documents leaked by the NSA whistle-blower Edward Snowden confirmed the news. Snowden files showed billions of data secretly acquired by the American agency after they carried intelligence gathering activities in India. The American agency used two of its secret data gathering programs – Boundless Informant and PRISM. The first one intercepts telephone calls and monitors internet activities within India whereas the latter secretly stole billions of data from various web-service providers such as Google, Microsoft, Yahoo, Apple and social networking sites such as Facebook and others.

After two days of 'The Hindu' news report, 'The Guardian' (Burke, 2013) brought out a similar report which revealed that NSA was not only spying on India but also on the Indian Embassy in Washington and the office of India's Mission to UN in New York. The documents leaked by Snowden demonstrates the degree and nature of hostility of datamining practices by the U.S. targeting its South Asian ally. These events were the wake-up calls for India to safeguard itself from illegitimate snooping and spying by foreign countries which could be extremely hostile in nature. India needed a comprehensive framework and a plan of action to tackle any sort of malicious cyber activities projected towards it.

4.3 Understanding the Policy

NCSP is a commendable step in the right direction taken by the government. The policy works as a stepping stone in enhancing the cyber security architecture of India. The study identifies seven different areas of interest where cyber policy will have a great impact.

a) Information and Communication Technology (ICT)

The cyber policy should be focused and dedicated towards R&D of the ICT sector. The policy should promote the culture of establishing research lab and institutions with the state-of-the-art digital infrastructure. A country should also have sound, effective and efficient technologies to counter any sort of malicious cyber activity.

b) Military & Defence

Cyber policy of a country is always in co-relation with the Military & Defence. Cyberterrorism and cyberwarfare are two major threats which every country faces now-a-days. It is important to keep the defence prepared. Military plays an important role in country's national security. But with changing times, wars are now fought on the cyber front rather than on the battlefields. It is crucial for a country to have a cyber army which looks into the issues related to cyber espionage, spying and intelligence data gathering.

c) Economy & Finance

The world is becoming a smaller place as e-commerce has revolutionized it. Countries are becoming hubs of investments that are made in the form of digital currency. Therefore, it is important that the cyber policy is effective enough to promote digital transactions and investment and at the same time safeguarding the economy. Cybercrimes and digital frauds are very common now-a-days and preventing and protecting against such dangers is one of the biggest challenges facing India.

d) E-governance & Human Resources

With the advancements in the technology, governments are looking towards e-governance for providing better services for public good. But this can only happen when a country has strong cyber security infrastructure. Managing and training skilled workers to prepare a robust cyber workforce who can attack, prevent and defend critical infrastructure of the country is also important. A well drafted cyber policy should address the methods, strategies and establishments for managing the country's cyber workforce.

e) Safeguarding information and privacy of the individual

The topmost priority of cyber policy of a country should be safeguarding the information and interest of the individuals along with their right to privacy. It is well known that people do not like their personal space to be encroached in the name of national security. A well-drafted cyber policy should thus respect the fundamental rights of its citizens while safeguarding their interests against any malicious cyber activity.

f) Public Private Partnership (PPP)

Private entities are the key stakeholders in the cyber domain, especially when it comes to cyber security solutions. They provide assistance to big business houses, multi-national companies, banks, and other e-commerce related entities. Technologies such as cloud computing is helping companies in providing easy access to product and services and also the ease of doing business with their clients and customers. But with increased opportunities, there comes the grave danger of cyber threat and cyber-attack to their businesses. There is a need to increase the public private partnership in the field of information technology along with various stakeholders. Cyber policy facilitates such discussions and debates and provides a way forward for vital partnerships.

g) International Cooperation on Cybersecurity

The inter-state relations are immersed in securing their economic stability and maintaining national security. There exists no balance of power in the cyber world, and cyber-attacks seem to have enough potential to convert the security dilemma of states into real acts of aggression. Therefore, such an understanding of events demands a strong international cooperation. A well drafted cyber policy promotes a strong sense of international cooperation with respect to matters concerning cyber activities. A brief understanding of cyberterrorism, cyberwarfare and cyber espionage is required to bring camaraderie among the countries.

4.4 Brief Analysis of NCSP 2013: The Shortcomings

a. Ambiguous Nature of the Policy

i. The Unresolved Dilemma

NCSP derives many of its objectives from the U.S. cyber security policy (DSCI, 2013). One of the aspects of the policy is considered to be economy driven approach, which means that the policy favours various business houses and other stakeholders by encouraging them to adopt cyber security practices as per their needs and requirements. Such an approach is criticized on the grounds that such practices do not support national security and becomes one of the major drawbacks in implementation of cyber policy. The NCSP is struggling with a dilemma to adopt either Economic driven or Legislation driven approach. On the one hand it talks about supporting organizations to adopt healthy cyber security practices and appoints various authorities to monitor and look after the cyber security needs of the organizations and keep a timely assessment report of the operationality of security measures and also provides them with fiscal schemes and incentives (MeitY, NCSP, 2013). Whereas on the other hand, it says that the companies should keep mandatory audit reports for all cyber security solutions and preparedness practices along with evaluation of effectiveness of information infrastructure (MeitY, NCSP, 2013). The policy does not specify or define what is meant by "Information Infrastructure"? Likewise, it is not specific on what kind of fiscal schemes and incentives is the government offering? What are the various criteria so that a company or business entity can avail these incentives? Are there any terms and conditions with respect to the sector to which the particular business belongs?

ii. Taking a Stance

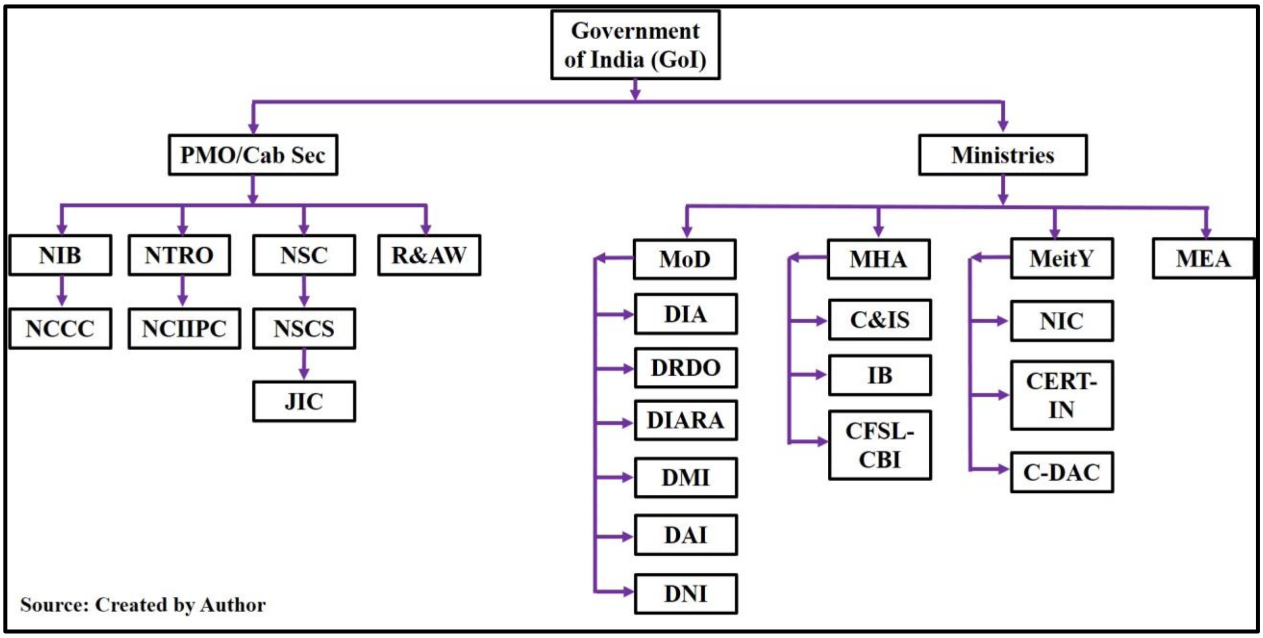
NCSP lacks transparency on information sharing and cooperation (MeitY, NCSP, 2013). It talks about developing bilateral and multilateral relationships but does not clearly specify what role India wants to play at the global level. India, being the seventh largest economy in the world, largest exporter of IT product and services and second largest internet users' base after China, should create more opportunities for becoming a global leader in the cyber world. The policy should mention initiatives and other plan of actions.

iii. The Evergreen Debate

NCSP triggers the classic debate of Right to Privacy versus National Security. The policy does not talk about methods and techniques used for data collection and other practices. It does not mention techniques regarding safeguarding the public interests. In the entire policy there is only one point which talks about safeguarding privacy of the citizens from cyber fraud or data theft leading to economic loss (MeitY, NCSP, 2013).

The policy does not talk about which organizations will be responsible for monitoring purposes.

b. The Organizational Overlap Figure 4.4: Current Cyber Organizational Structure in India (Source: created by Author)



Source: Created by Author

NCSP is a national cyber policy of India but does not talk about any government organization which looks into the issues concerning cyber security. It is considered to be one of the biggest drawbacks of the policy. Despite this, there are a number of organizations which are monitoring the cyber ecosystem of India.

From the organization diagram, it can be easily concluded that there are multiple agencies monitoring the cyberspace of India which makes it really complex at times of implementation of law and order and decision making (Chhabra, 2013).

1. Cyber Security Architecture Tier 1 (Under PMO)

There are currently eight apex agencies under the PMO that are working with the matters related to cyber security. Out of eight, six of them are completely dedicated towards safeguarding the cyber security architecture in India. These six bodies are:

i) National Information Board (NIB) – policy making body on cyber security.

ii) National Cyber Coordination Centre (NCCC) – works under NIB responsible for e-surveillance in India.

iii) National Technical Research Organization (NTRO) – dedicated Technical intelligence agency of India.

iv) National Critical Information Infrastructure Protection Centre (NCIIPC) – an extended unit of NTRO works for securing critical infrastructure of the country.

v) Joint Intelligence Committee (JIC) – works under National Security Council Secretariat (NSCS) in close coordination with other external agencies.

vi) Research and Analysis Wing (R&AW) – India's external intelligence agency also looks after cyber threats or attacks from foreign land.

2. Cyber Security Architecture Tier 2 (Under Ministries)

There are twelve regulatory bodies working under four ministries dealing with cyber security within as well as outside the country. They are:

i) Ministry of Defence (MoD) – Under MoD, there are organizations like Defence Intelligence Agency (DIA), Directorate of Military Intelligence (DMI), Directorate of Air Intelligence (DAI), Directorate of Naval Intelligence (DNI), Defence Information Assurance and Research Agency (DIARA), Defence Research and Development Organization (DRDO) working in gathering intelligence and monitoring cyber activities.

ii) Ministry of Home Affairs (MHA) – Under MHA, there are organizations like Cyber and Information Security (C&IS) division, Intelligence Bureau (IB) and Central Forensic Science Laboratory (CFSL) – CBI division which are focusing on internal cyber security settings along with cyber forensics.

iii) Ministry of Electronics and Information Technology (MeitY) – Under MeitY, organizations like National Informatic Centre (NIC), Indian Computer Emergency Response Team (CERT-In), Centre for Development of Advanced Computing (C-DAC) responsible for developing state of the art technologies for monitoring cyber activities.

iv) Ministry of External Affairs (MEA) – Under MEA, Ambassadors, High Commissioners, Defence attaché from various Indian Armed Forces, and Joint Secretaries (IT) look after the state of cyber security.

3. The Parallel Hierarchical Disorder

If both the Tiers of Cyber Security Architectures are combined, 22 organizations would work to safeguard the cyberspace. But the question raises, is each one of them doing a commendable job? Such an overlapping organizational structure creates confusions and hampers the effectiveness and productivity of result-oriented works.

4. Who is Responsible?

These 22 apex bodies, organizations and initiatives under four ministries are headed by officials with high ranking authorities. It comprises of the NSA, Secretaries, Joint Secretaries, Army Generals, Air Marshals, Rear Admirals, Former Director Generals of Police (DGPs), senior most bureaucrats, retired bureaucrats and other specialized and distinguished experts from various fields. (refer Table 5.4.1). With such a nexus of high-ranking officials, it brings disequilibrium among the functioning of various organizations.

5. The MEA factor

The MEA's entry has made the situation all the more complex. MEA is responsible for engaging with foreign countries and managing relations with them. But now MEA is also taking a lead in handling the matters of cyber security in the international arena. India-US Cyber security Forum is already in progress. According to MEA factsheet (MEA, 2006), India's CERT-In and US's National Cyber Security Division have already signed an agreement. The document also talks about cooperation between India's Standardisation Testing and Quality Certification (STQC) and US's National Institute of Standards and Technology (NIST). As a matter of fact, both CERT-In and STQC comes under the jurisdiction of MeitY but the document fails to mentions anything about MeitY.

c. Other Major Shortcomings of NCSP

i. The policy fails to talk about IT Act 2000 all-together. In case of any conflict, IT Act will always prevail as the cyber policy is just a roadmap.

ii. It does not mention roles and responsibilities of various stakeholders for implementation of policy objectives.

iii. The policy talks about creating a cyber workforce of 500,000 professionals in the next 5 years but it does not clarify the functions, roles and responsibilities of such a workforce (MeitY, NCSP, 2013). In fact, according to IBM, as of 2018 there is a shortage of 3 million cyber security professionals in India (PTI, 2018)

iv. The policy also talks about developing indigenous products for cyber security in order to reduce dependence on global supply chain (MeitY, NCSP, 2013). India first needs to develop high testing technologies in order to meet the desired global standards. In order to make such technologies, India will need to rely on the global supply chain which counters the whole essence of the objective about reducing global supply chain.

Table 4.4: India's Premier Cyber Organizations with Ranks of Officials heading them. (Source: created by Author)

India's Premier Cyber Organizations						
Organization(s)/ Authorities	Prime Minister's Office (PMO)/ Cabinet Secretariat (Cab Sec)	Ministry of Defence (MOD)	Ministry of Home Affairs (MHA)	Ministry of Electronics & Information Technology (MeitY)	Ministry of External Affairs (MEA)	Rank(s) of the Head of the organization
National Information Board (NIB)	✓					National Security Advisor (NSA)
National Security Council (NSC)	✓					National Security Advisor (NSA)
National Cyber Coordination Centre (NCCC)	✓					Specialised Expert (PhD)
National Technical Research Organization (NTRO)	✓					Senior Most IPS Officer or Former DGP
National Critical Information Infrastructure Protection Centre (NCIPC)	✓					Specialised Expert (PhD)
Joint Intelligence Committee (JIC)	✓					Senior Most IPS Officer or Former DGP
Research and Analysis Wing (R&AW)	✓					Senior Most IPS Officer or Former DGP
Defence Intelligence Agency (DIA)		✓				Lt Gen
Defence Research and Development Organization (DRDO)		✓				Scientist (E)
Defence Information Assurance and		✓				Maj Gen

Research Agency (DIARA)						
Directorate of Military Intelligence (DMI)		✓				Maj Gen
Directorate of Air Intelligence (DAI)		✓				Air Vice Marshal
Directorate of Naval Intelligence (DNI)		✓				Rear Admiral
Cyber and Information Security (C&IS) division			✓			Joint-Secretary (IT)
Intelligence Bureau (IB)			✓			Senior Most IPS Officer or Former DGP
Central Forensic Science Laboratory (CFSL) – CBI			✓			Specialised Expert (PhD)
National Informatics Centre (NIC)				✓		Specialised Expert (PhD)
Indian Computer Emergency Response Team (CERT-In)				✓		Specialised Expert (PhD)
Centre for Development of Advanced Computing (C-DAC)				✓		Specialised Expert (PhD)
Ambassadors and High Commissioners					✓	Senior Most IFS officer
Defence Attachment(s)					✓	Lt Col and Equivalent
Cyber Security Initiatives					✓	Joint Secretary (IT)

-

Chapter 5
The Fading & Failing Policy

This chapter is aimed at linking the policy shortcomings with the increasing number of cyber security incidents every year. For data collection, Indian Computer Emergency Response Team (CERT-In) Annual Reports (2006-17) were collected and analysed. CERT-In is a national nodal agency that deals with cyber security threats like hacking and phishing. It is a division that comes under the aegis of MeitY.

Every year CERT-In brings out a brief annual report describing the overall security scenario of that particular year. The data for this paper has been compiled from CERT-In reports starting from the year 2006 up till 2017. It has been argued that there is a dire need to strengthen our cyber security defence and to revise the NCSP.

5.1 Increasing Cyber Security Incidents

The data suggest that there is a significant increase in number of cyber security incidents. The number of incidents was at the peak during 2013-14, the same time when the NCSP was made public. These incidents include Website Intrusion & Malware Propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements and Unauthorized Scanning activities (CERT-In, 2006-17).

5.2 Indian Website Defacement Incidents

Website Defacement is a type of malicious cyber-attack where a hacker hacks into a server and changes the look of the targeted website, changing the appearance of the website or the webpage. It basically means drawing graffiti on the wall but virtually. According to some studies (PTI, 2008), the main objective behind website defacement is propagating political agenda or ideologies. According to the CERT-In statistics, there is a significant increase in the number of incidents of Indian website defacement. In 2018, the Ministry of Defence website was defaced. Officials reported that there were Mandarin characters all over the website indicating that Chinese hackers may have been behind it (Goswami, 2018).

5.3 Bot Infected System

This is one of the most dangerous cybercrimes. Bot or Bot-net is made up of two words consisting of 'Robot' and 'Network'. A Robot is anything which functions automatically and performs certain set of commands or obeys orders whereas a Network is group of systems linked together. It becomes difficult to manually operate a computer system which is infected by malicious codes. Therefore, hackers use Bot or Botnet which makes it easier to operate a set of systems connected to a network infected with a malicious code. The number of botnet incidents has been gradually on the rise in India and were maximum in the years 2008, 2010, 2016 and 2017.

5.4 Incidents of Phishing

Phishing is used by hackers to steal crucial information such as credentials, banking details, usernames, passwords and other sensitive data. The perpetrators disguise themselves as legit entity or authority and demand information from the user. According to the CERT-In, phishing incidents were maximum in 2014 (close to 1122).

5.5 Incidents of Virus/ Malicious Code

This refers to wide variety of malicious program that can cause severe damage to the computer. These include computer viruses, worms, trojan horse and various other potential software which can disrupt or destroy the digital infrastructure. According to CERT-In data, such incidents are increasing at a significant rate and maximum number of incidents were reported in 2014 and then in 2016.

5.6 Incidents of Spam

Spam usually refers to any unsolicited electronic mail for which the user has not signed up or registered. Spam are generally unwanted emails with malicious code or virus and tend to lure users with false advertisements and promises. Most of the spams are related to money fraud. Spams usually promote phishing and email fraud. CERT-In statistics reveal that the number of spam incidents (close to 85,659) was maximum in 2014.

5.7 Incidents of Website Comprise & Malware Propagation

With increase in number of cyber-attacks, Indian websites are becoming more and more vulnerable to malware propagation. There is a significant increase in compromise of Indian websites. Most of the targeted websites are of government domain or banking facility. According to CERT-In statistics, during 2008-09 and 2013-14, there was rapid increase in number of such incidents.

5.8 Incidents of Network Scanning/ Probing

In order to trace malicious activities over the internet, CERT-In has set up a dedicated facility which monitors the network traffic over the internet. Since internet is such a huge domain and scanning everything on it is difficult and tedious, many organizations voluntarily provide data and information regarding their network traffic. Information collected through this scanning process is extremely beneficial since it helps in issuing timely advisories and send alerts to various organizations. These organizations then take adequate steps and adopt methods and techniques which further help them in safeguarding their data and information. According to CERT-In stats, till now a very large volume of network traffic has been scanned. But there has been a gradual increase from 2016.

5.9 Analysis of Combined Cyber Security Incidents (2006-17)

The Indian Cyberspace is mostly infected by Spams, followed by incidents of Virus/Malicious code, phishing, incidents of Website Compromise and Malware propagation. Most of the malicious activities are conducted via Spam emails. In most cases, spam mails consist false information about winning a lottery, jackpot, or becoming a millionaire overnight. The perpetrator on the pretext of such information asks for personal details of the user mainly credentials and banking information. Furthermore, spam leads to malicious activities like phishing and infecting system or network with a virus or a malicious code. The best advisories issued from CERT-In is that when in doubt, never click on links from an unsolicited mail, under any circumstances never download files from any suspicious mail and the most important thing never ever share your password.

5.10 Cyber Security Response Activities by CERT-In

Every year, CERT-In issues security alerts, vulnerability notes, advisories and organize cyber security training for professionals to help organizations prepare action-prevention plan for countering any sort of cyber threat or attack. The objective of trainings is to train the skilled workforce in identifying various threats and challenges in the cyber domain and be prepared for any sort of emergency situations.

5.11 Cyber Attacks from Foreign Countries

According to CERT-In reports (India Today Webdesk, 2018), it has identified various countries from where many cyber threats or attacks have originated and diverted towards India. Majority of cyber-attacks on official websites of India is from China with 35% attacks originating from there. Followed by USA with 17%, Russia 15%, Pakistan 9%, Canada 7%, Germany 5%, Netherlands 4%, North Korea and France with 2% each.

The attacks were made on the official websites of Indian government and other public sector entities. The attacks include phishing, spamming, espionage and website defacement. Indian companies that are mostly affected by these attacks were Oil and Natural Gas Corporation (ONGC), National Informatics Centre (NIC), Indian Railways Catering and Tourism Corporation (IRCTC) and Centre for Railway Information Systems (CRIS). Some of the largest public sector banks in India such as Punjab National Bank (PNB), Oriental Bank of Commerce (OBC) and State Bank of India (SBI) were also severely disturbed from these cyber-attacks.

According to International Telecommunication Union's (ITU) Global Cybersecurity Index (GCI) Annual report for the year 2017, India is at 23rd rank among the list of 165 nations (ITU, 2017) on the level of commitment of individual countries towards cyber security. India had a score of 0.683 and is categorized under the "maturing" section. ITU is a specialized agency of the UN looking into the matter of information and telecommunications technologies at a global level. There are total 77 countries along with India in the "Maturing" category (i.e., GCI score between the 50th and 89th percentile) that have complex commitments, and engage in cybersecurity programmes.

The index shows that India is not yet a cyber mature nation and is not ready for any sort of major cyber threat or attack. India needs a strong, resilient National Cyber Security Policy. The cyber response activities are not effective enough to retaliate or stop an attack completely. It's thus time to take some concrete steps and revise the cyber policy to make it more relevant.

5.12 Research Findings

a. Cybersecurity is one of the primary concerns when dealing with matters related to national security.
b. There is a crucial need to opt for enhanced international cooperation on the matters of cyber security.
c. Cyberwarfare is the future of war and it can only be avoided when states are well equipped with cyber technologies. There is a significant need to establish a balance of power in the cyber domain.
d. Illegitimate use of cyber technologies by various non-state actors is increasing, which can be termed as an act of cyberterrorism.
e. There is a crucial need to establish a dialogue between various stakeholders, such as academia, corporate houses, banking sector, financial service providers, organizations providing cyber security services and solutions, and the government bodies dealing with the matter of cyber security.

f. A strong nexus is required between the public and private sector. Government should encourage more private entities to invest in cyber security services and promote a safe, secure and resilient cyberspace.

g. E-commerce, E-governance and E-surveillance all require a secure cyberspace in order to provide effective services.

h. Cyber security should be absorbed in the curriculum of schools, colleges and universities.

i. The percentage of Cyber Security Awareness is very low in India. People lack basic cyber ethics and manners of code and conduct while surfing internet.

j. Every year, number of cyber security incidents are increasing at a significant rate and is jeopardizing both the personal data and information of individuals and national security.

Figure 5.1: Cyber Security Incidents Reported by CERT-In (2006-17) (Source: CERT-In Reports; compiled by Author)

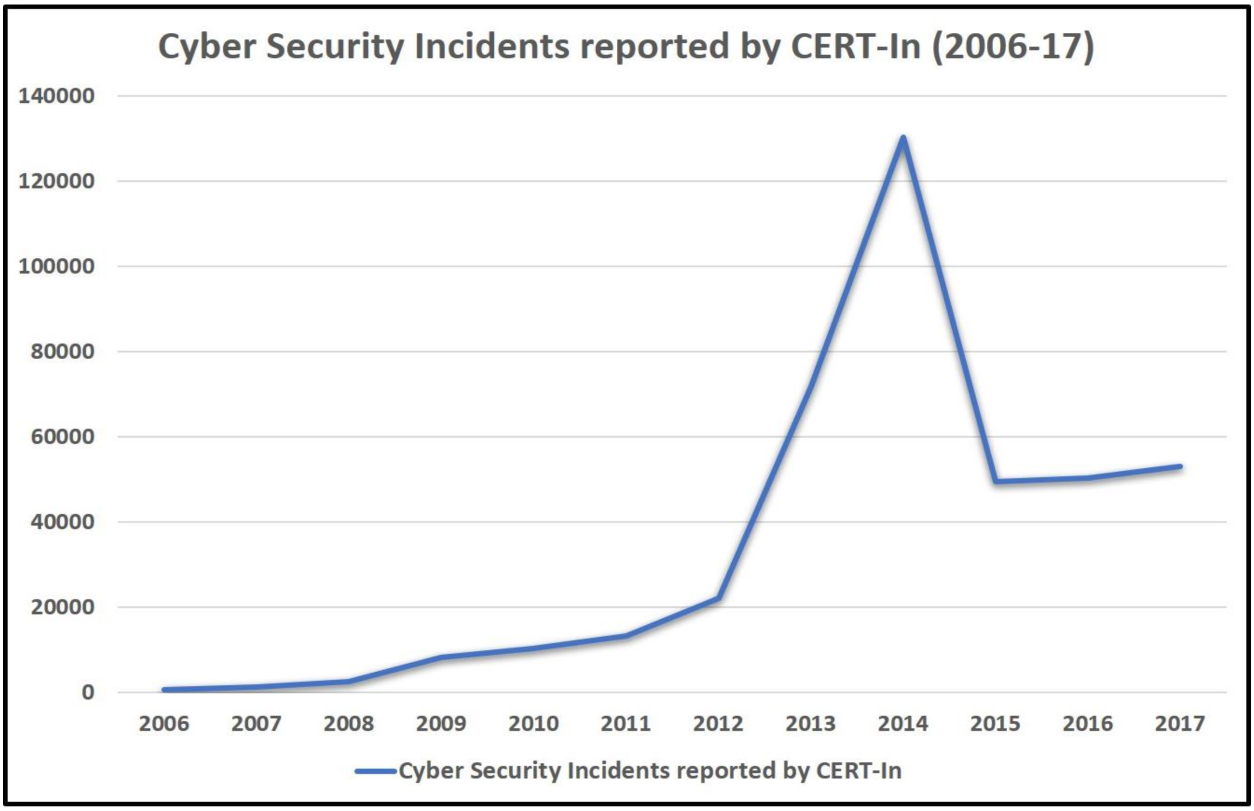


Figure 5.2: Indian Website Defacement tracked by CERT-In (2006-17) (Source: CERT-In Reports; compiled by Author)

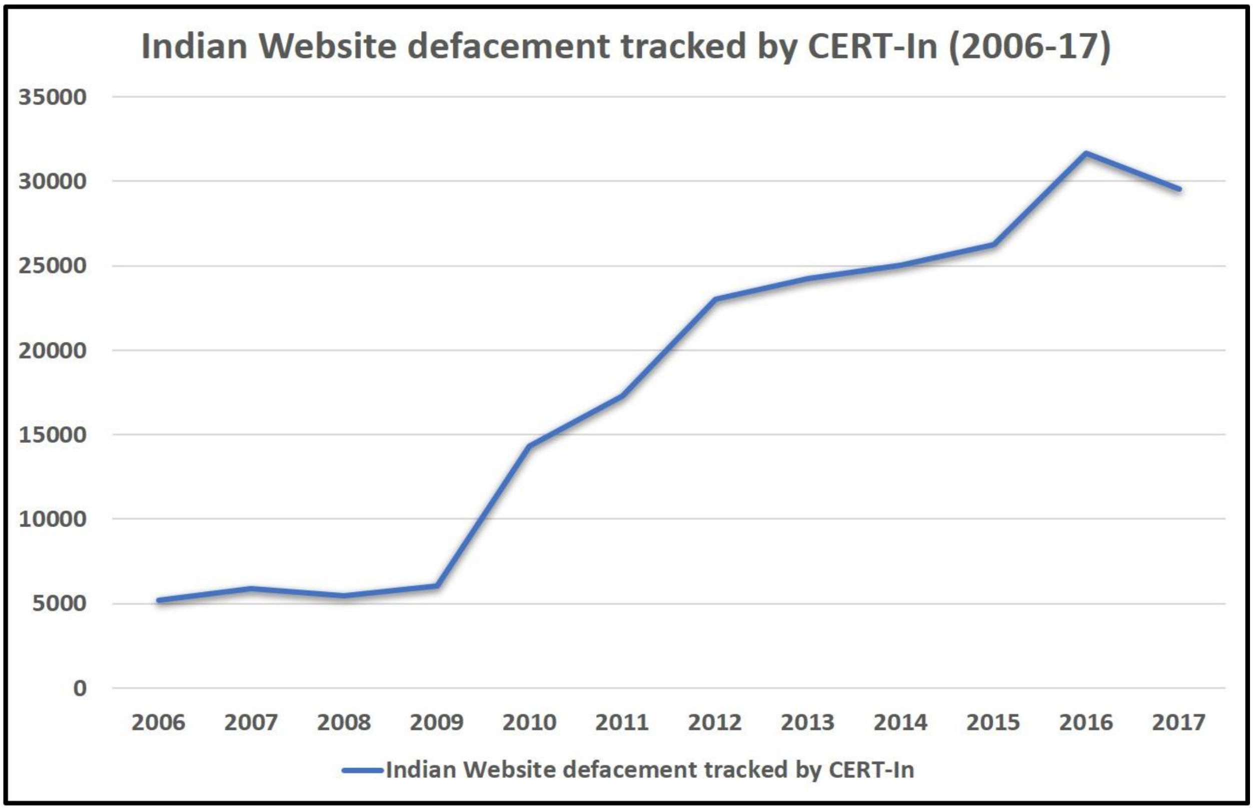


Figure 5.3: Bot Infected System tracked by CERT-In (2006-17) (Source: CERT-In Reports; compiled by Author)

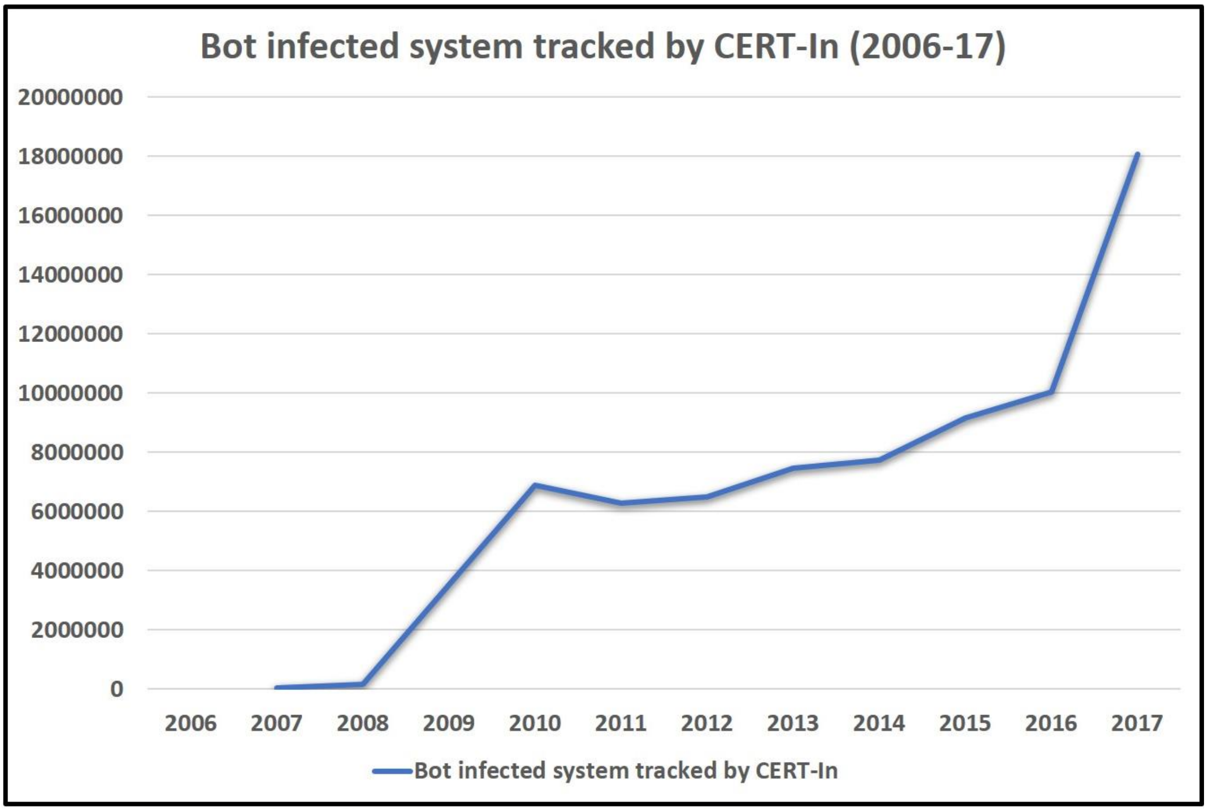


Figure 5.4: Incidents of Phishing reported by CERT-In (2006-17) (Source: CERT-In Reports; compiled by Author)

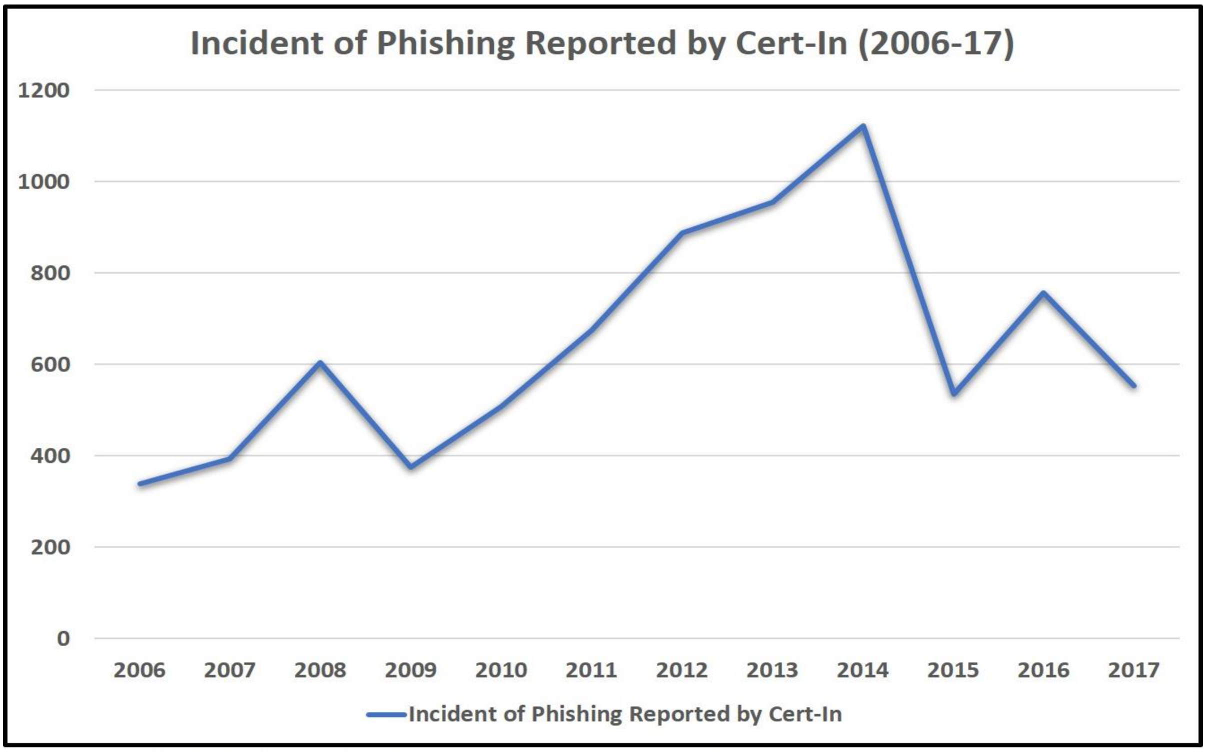


Figure 5.5: Incidents of Virus/ Malicious Code reported by CERT-In (2006-17) (Source: CERT-In Reports; compiled by Author)

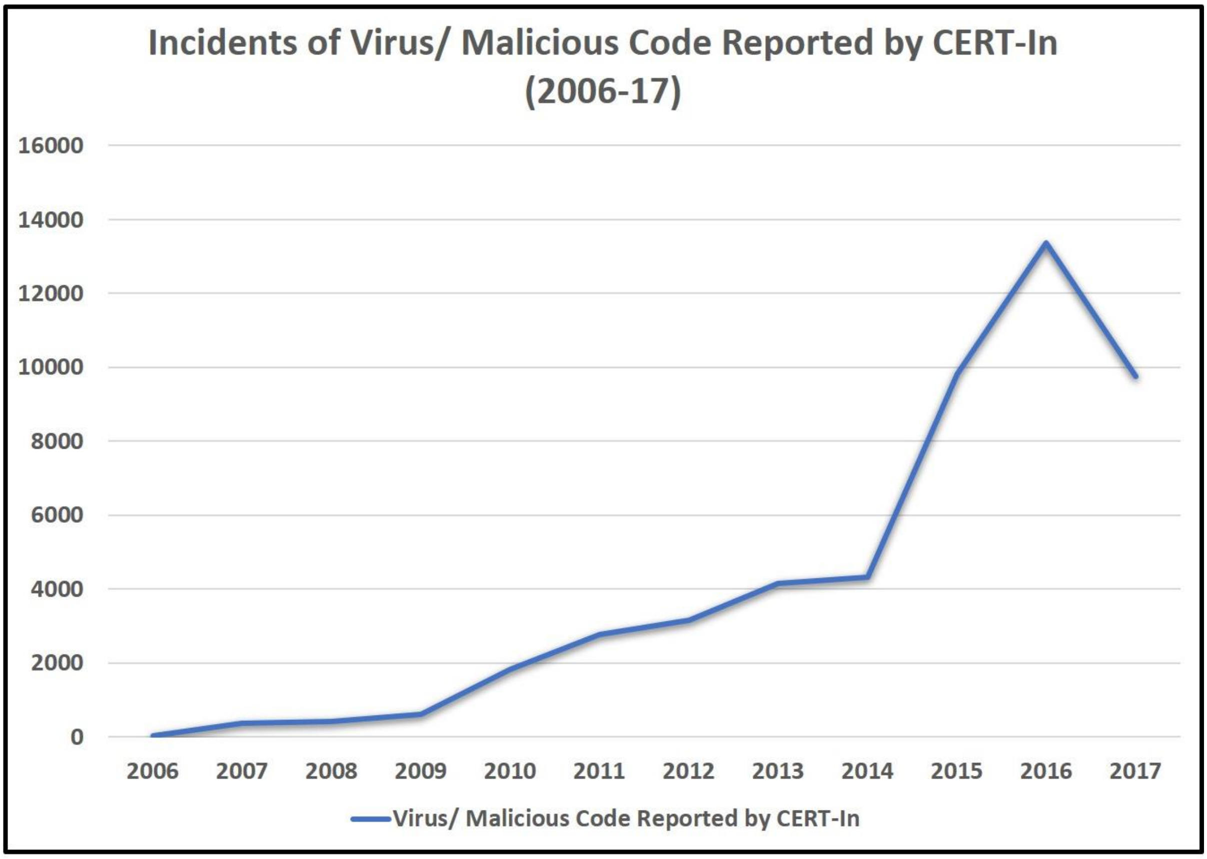


Figure 5.6: Incidents of Spam reported by CERT-In (2006-17) (Source: CERT-In Reports; compiled by Author)

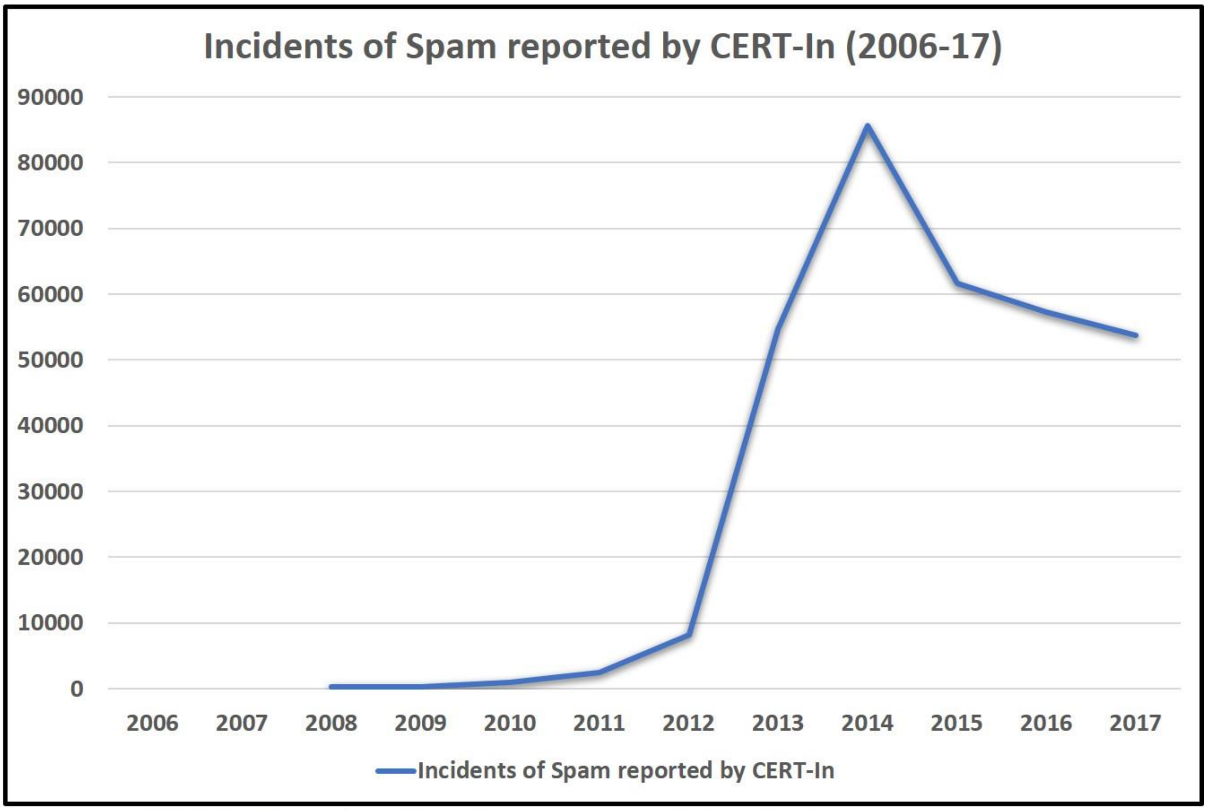


Figure 5.7: Incidents of Website Compromise & Malware Propagation (Source: CERT-In Reports; compiled by Author)

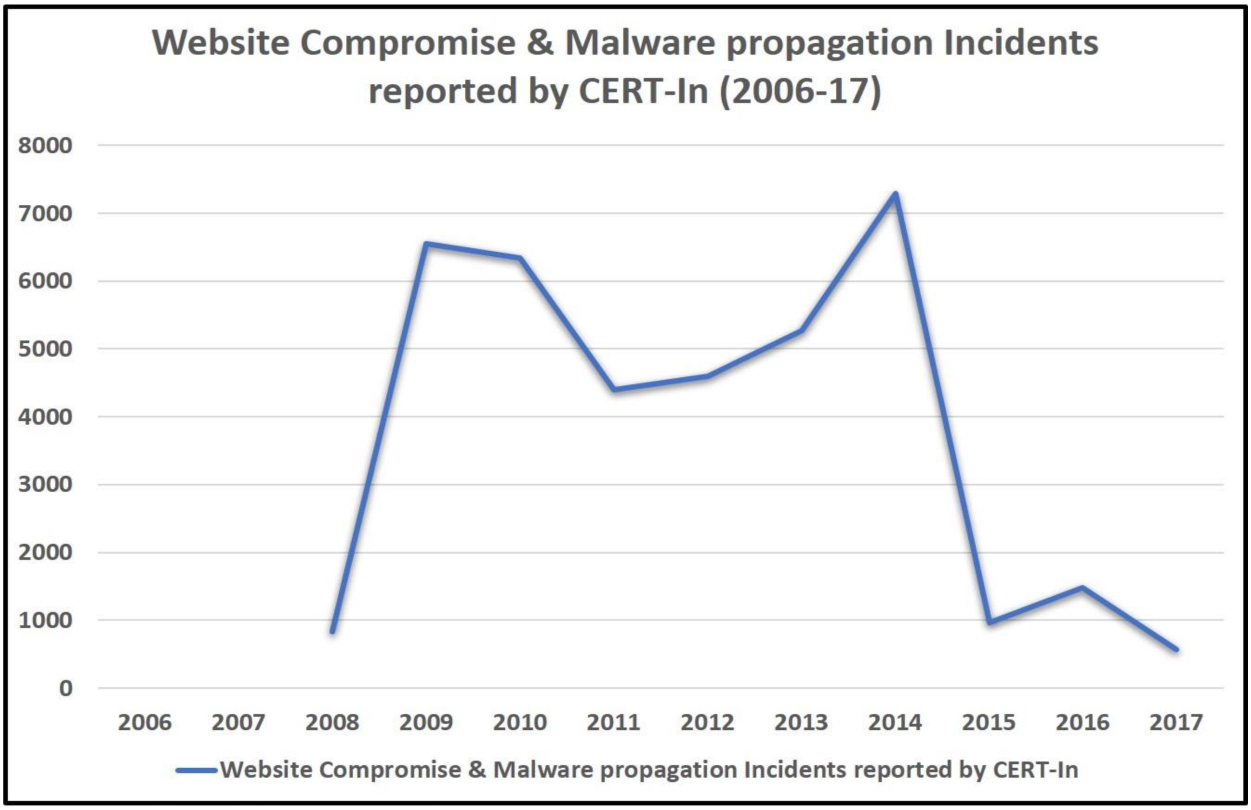


Figure 5.8: Incidents of Network Scanning and Probing (Source: CERT-In Reports; compiled by Author)

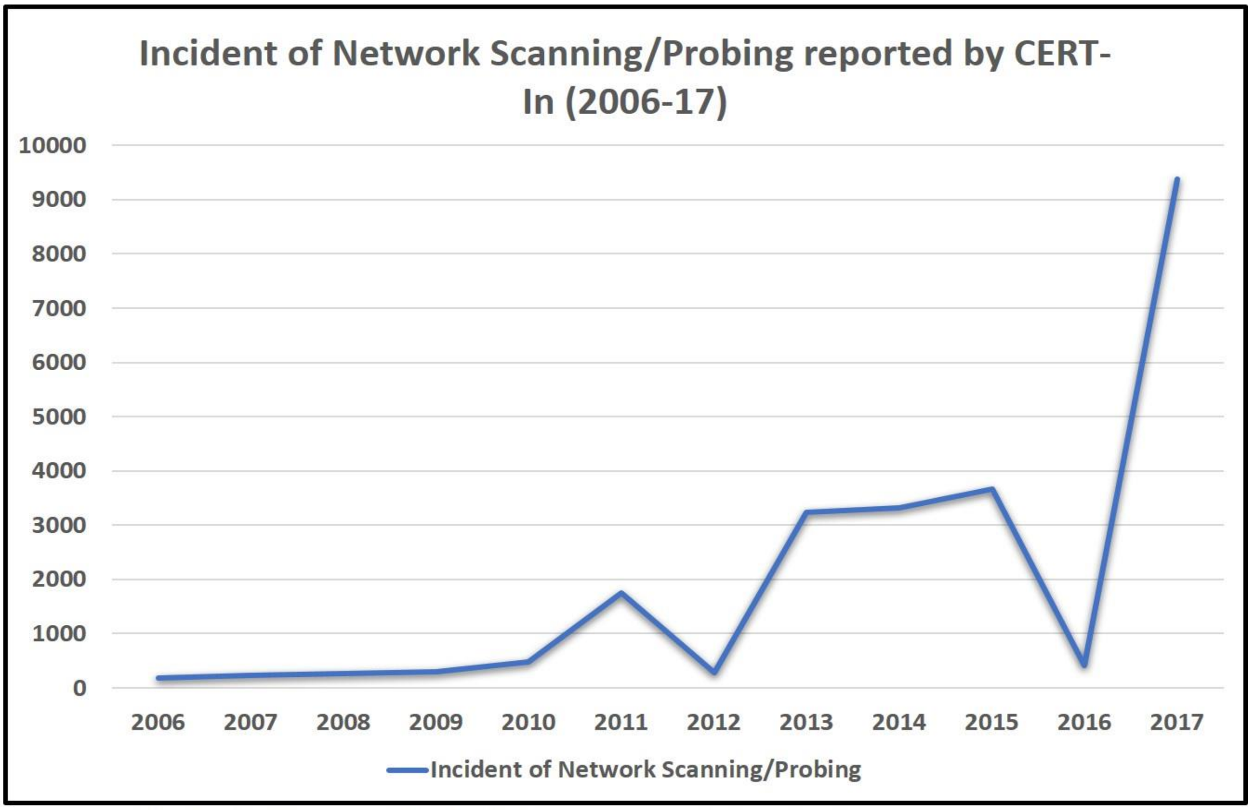


Figure 5.9: Analysis of Combined Cyber Security Incidents (2006-17) (Source: CERT-In Reports; compiled by Author)

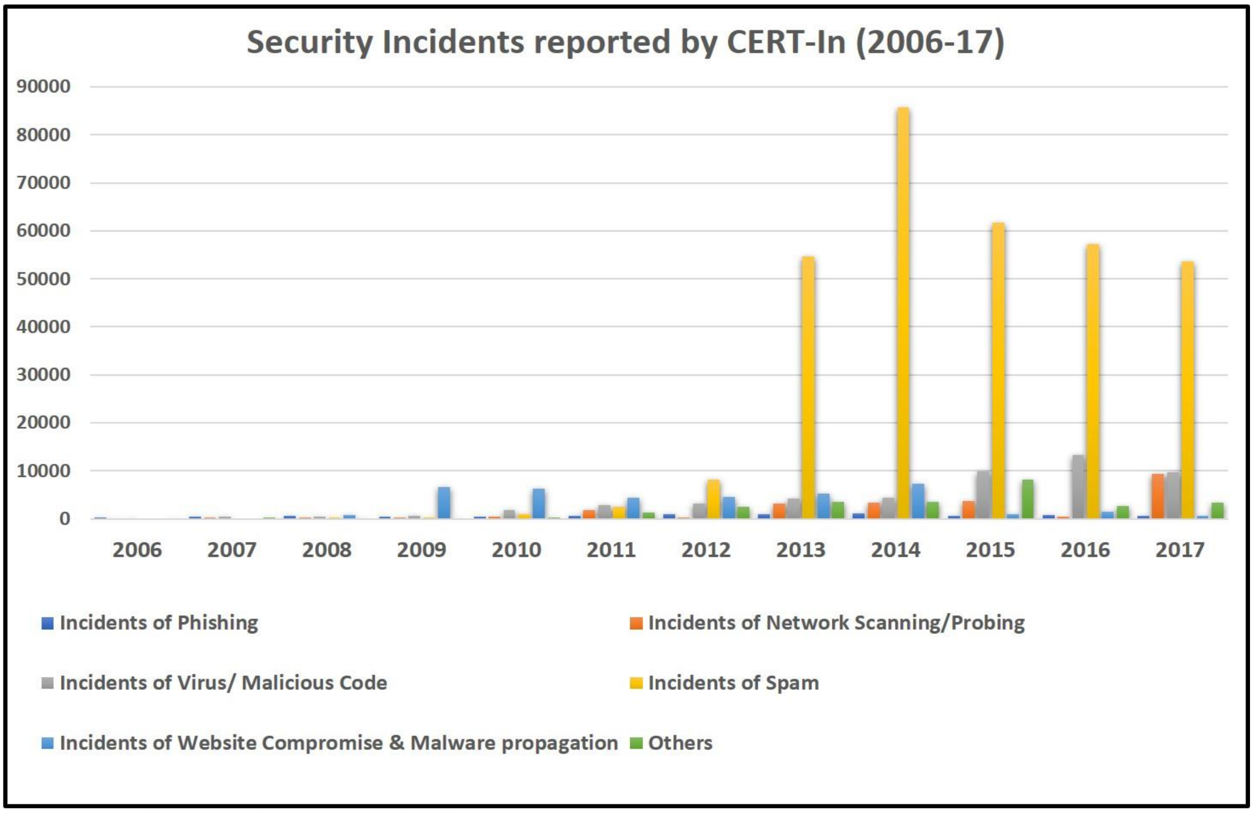


Figure 5.10: Cyber Security Activities Reported by CERT-In (2006-17) (Source: CERT-In Reports; compiled by Author)

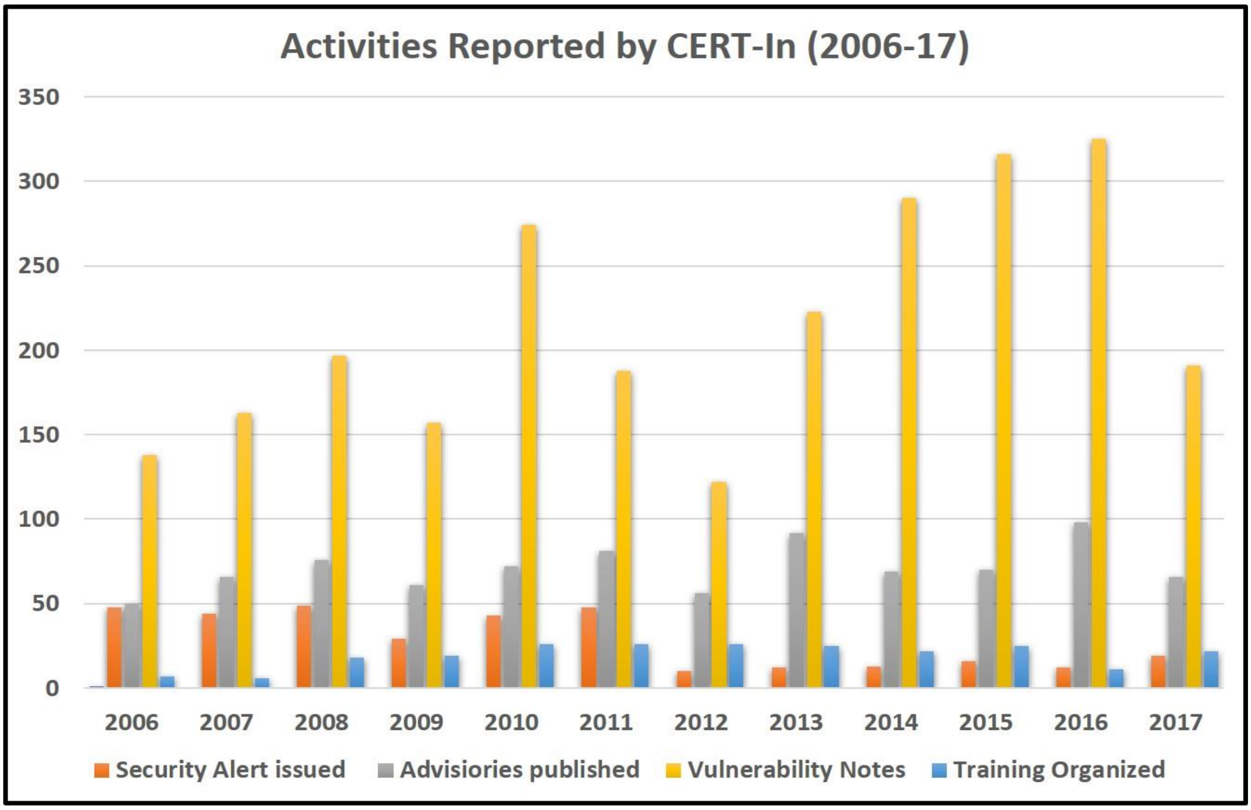
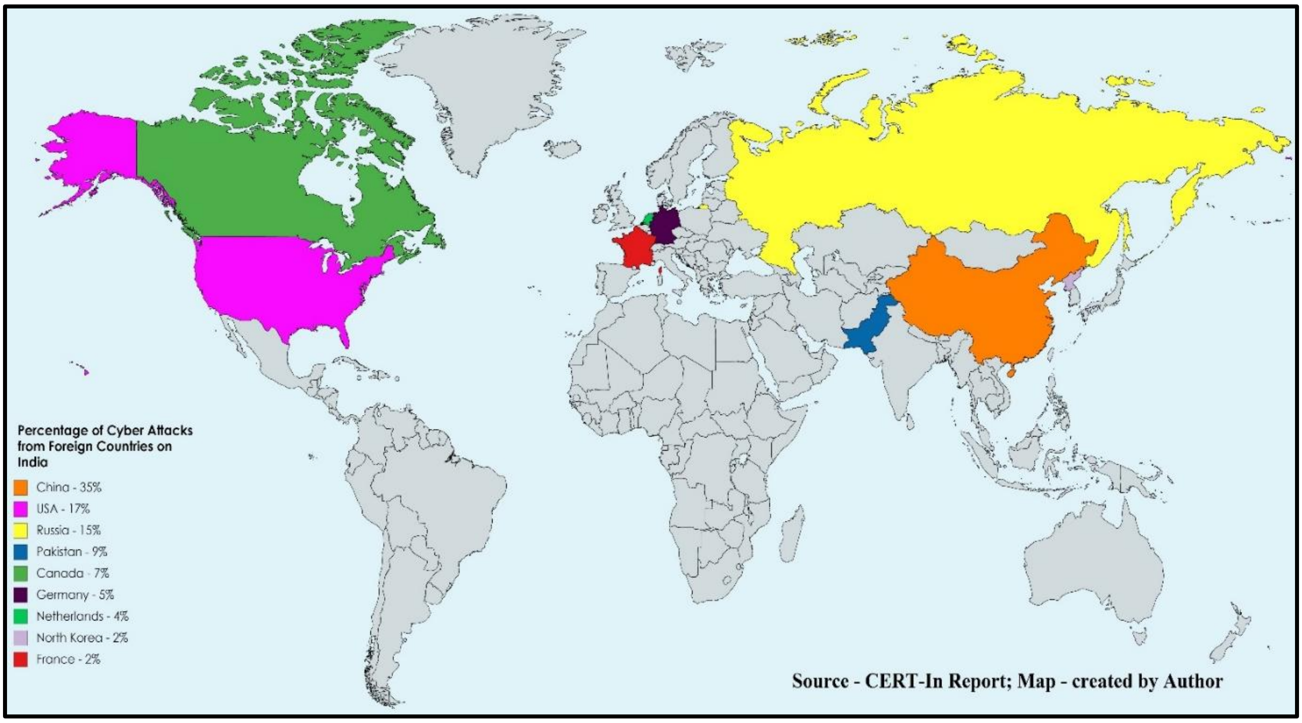
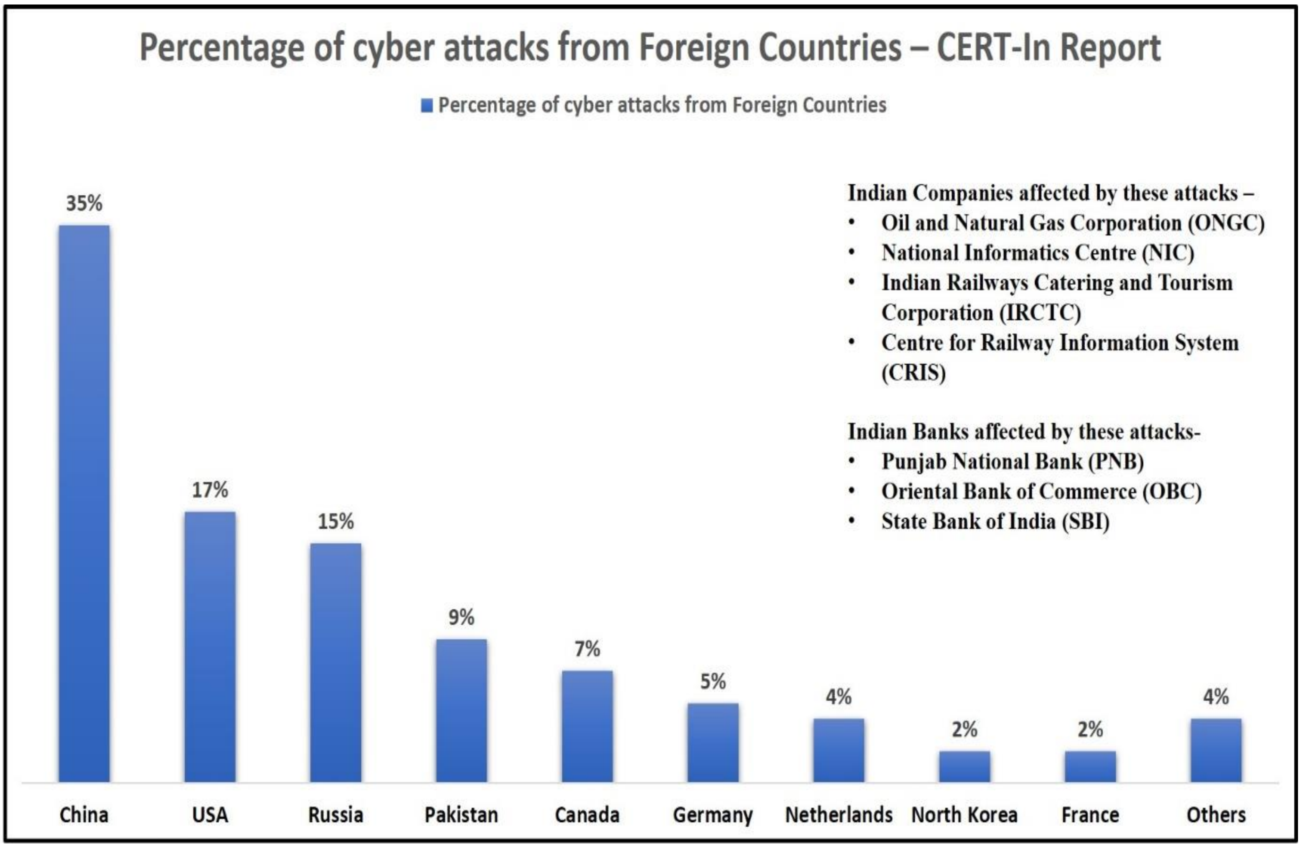


Figure 5.11.1: Percentage of Cyber Attacks on India originating from Foreign Countries (Map) (Source: CERT-In Reports; compiled by Author)



Source - CERT-In Report; Map - created by Author

Figure 5.11.2: Percentage of Cyber Attacks on India originating from Foreign Countries (Graph) (Source: CERT-In Reports; compiled by Author)



Indian Companies affected by these attacks –

- Oil and Natural Gas Corporation (ONGC)
- National Informatics Centre (NIC)
- Indian Railways Catering and Tourism Corporation (IRCTC)
- Centre for Railway Information System (CRIS)

Indian Banks affected by these attacks-

- Punjab National Bank (PNB)
- Oriental Bank of Commerce (OBC)
- State Bank of India (SBI)

Table 5.9: CERT-In Reports Data – Cyber Security Incidents (2006-17) (Source: CERT-In; table created by Author)

CERT-In Report(s) Analysis – Security Activities (2006-17)							
Year	Security Incidents	Security Alert issued	Vulnerability Notes	Training Organized	Indian Website defacement tracked	Open Proxy servers tracked	Bot infected system tracked
2006	552	50	138	7	5211	1837	-
2007	1237	66	163	6	5863	1805	25915
2008	2565	76	197	18	5475	2332	146891
2009	8266	61	157	19	6023	2583	3509166
2010	10315	72	274	26	14348	2492	6893814
2011	13301	81	188	26	17306	3294	6277936
2012	22060	56	122	26	23014	2759	6494717
2013	71780	92	223	25	24216	2224	7457024
2014	130338	69	290	22	25037	2408	7728408
2015	49455	70	316	25	26244	1698	9163288
2016	50362	98	325	11	31664	-	10020947
2017	53081	66	191	22	29518	-	18077185

Table 5.10: CERT-In Reports Data – Cyber Security Incidents (2006-17) (Source: CERT-In; table created by Author)

CERT-In Report(s) Analysis – Security Incidents (2006-17)						
Year	Phishing	Network Scanning/Probing	Virus/ Malicious Code	Spams	Website Compromise & Malware propagation	Others
2006	339	177	19	-	-	10
2007	392	233	358	-	-	264
2008	604	265	408	305	835	94
2009	374	303	596	285	6548	145
2010	508	477	1817	981	6344	188
2011	674	1748	2765	2480	4394	1240
2012	887	286	3149	8150	4591	2417
2013	955	3239	4160	54677	5265	3484
2014	1122	3317	4307	85659	7286	3610
2015	534	3673	9830	61628	961	8213
2016	757	416	13371	57262	1483	2671
2017	552	9383	9750	53692	563	3315

Chapter 6

Recommendation and Conclusion

6.1 Organizational Restructure

There is a crucial need to restructure the current government organizational setup. As stated, there are more than 22 bodies in the field of cyber security. This often causes work overlap and overlooking of serious matters. Given below is the proposed organizational setup consisting of one Tier cyber security architecture with 7 organizations:

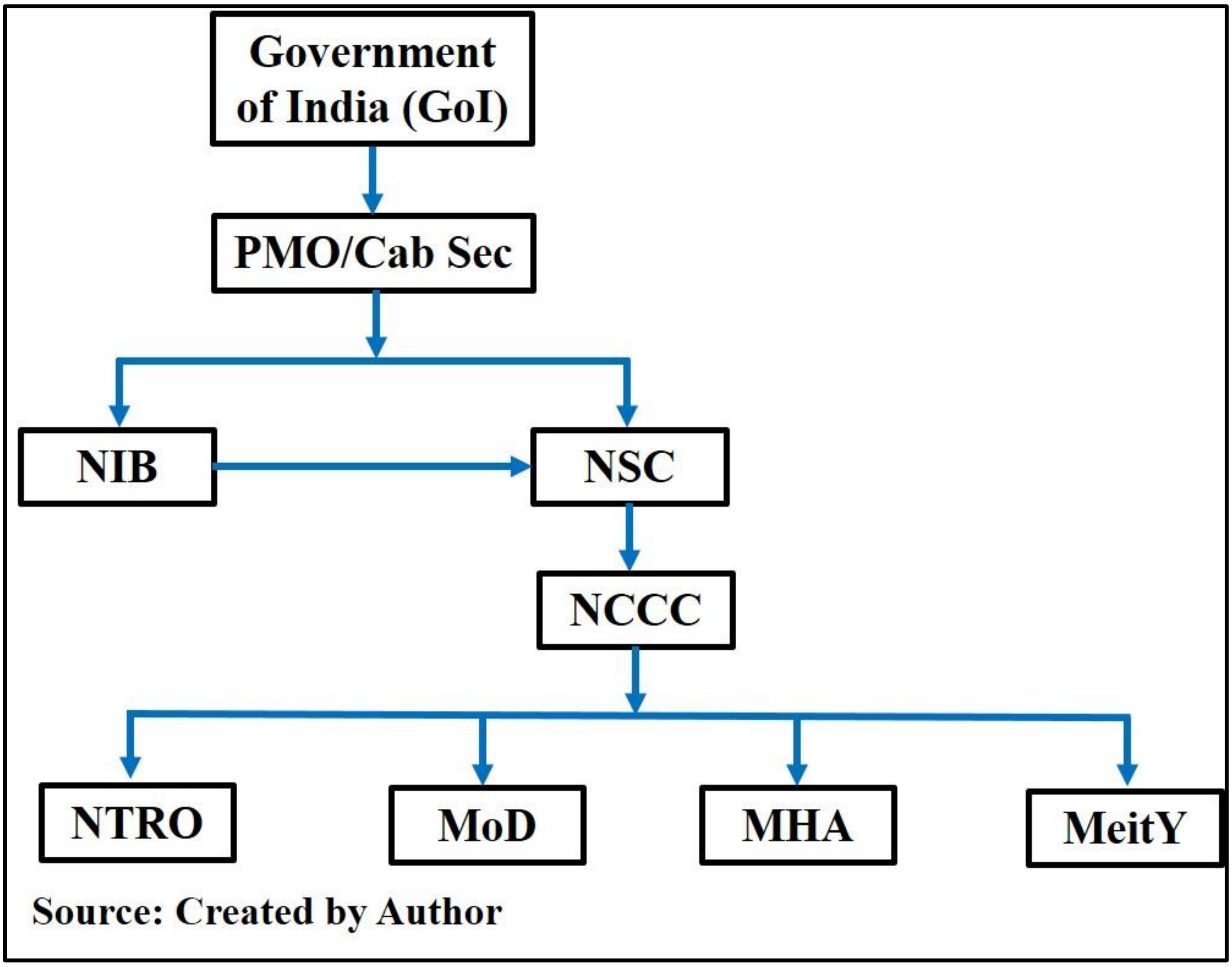


Figure 6.1: Proposed Cyber Organizational structure (Source: created by Author)

a) **Prime Minister's Office (PMO)** - The entire setup will be superintended by PMO for efficient and effective working of the organization.

b) **National Security Council (NSC)** – It will work as the overall governing and decision-making body on all matters related to cyber security of the country. It will be as usual under direct command of NSA.

c) **National Information Board (NIB)** – It will play a crucial role in policy formulation and providing recommendation to the NSC. The working strength of NIB should be reduced from 21 to maximum 6-7 members. As the chairman of NIB is the NSA, the deputy chairman should be a Secretary to the Government of India. The remaining should be advisory members of an advisory committee. The members should consist of officials from MoD, MHA, MeitY, MEA, Intelligence Agencies, NSC and Academia.

d) **National Cyber Command Centre (NCCC)** – NCCC should be renamed as "*National Cyber Command Centre*" which will be the supreme governing body looking after the cyber security of India. It will be an integrated cyber command centre working in close collaboration with other organizations and agencies. All other organizations and agencies will be answerable to NCCC Chairman who will be the member of NSC and will also be an advisory member of NIB. NCCC will oversee and monitor cyber activities. It will not engage or interfere in activities and responsibilities of premier intelligence agencies (NTRO, IB, and R&AW) other than the cyber aspect. It will be the premier body dealing with the matters of cyber security and e-surveillance in India. The ultimate aim of NCCC will be to integrate the entire cyber security setup of the country under a single organization.

e) **Other Organizations and Ministries** like NTRO, MHA, MoD and MeitY will look after the external cyber threats from foreign countries, internal threats and attack originating within the country, cyber threats and attacks critical to national security and development of indigenous cyber security technologies respectively.

f) All the above – mentioned organizations will provide particular data to NCCC which will further prepare a plan of action to safeguard the Indian cyberspace.

g) Establishing a new NCCC will ensure that a hierarchical structure is formed and each official is answerable. It will keep minute details and data intact.

h) NCCC will be responsible for initiating bilateral or multilateral engagements. For instance, NCCC will work in close coordination with MEA whereas MEA will represent Indian interests abroad and NCCC will ensure that the objectives of all international agreements are implemented.

6.2 Bridging the gap for Skill-development

a) Inculcating knowledge rather than education about cyber security

Indian education system lacks knowledge on cyber security. It is not included in school curriculum which results in students losing interest on the subject. Although young people are increasingly using internet, it can be a dangerous place without proper guidance. A survey conducted by National Cyber Security Alliance and Microsoft states that 91% of the teachers agree that cyber security should be taught in schools (Abhimanyu, 2017).

Also, Cyber bulling is one important concern for students on the digital domain. The "***Blue Whale Challenge***" is one such example which has created havoc in the recent years (Rossow, 2018). It is a suicide game where participants are given 50 days task and the last task is to commit suicide. The trick is that the game is completely hidden online and is only accessible to participants who are mentally depressed or are often bullied at schools. Close to 20 cases were reported in India, out of which 11 committed suicide and 9 somehow escaped but remained traumatized. This clearly highlights the gap in cyber security education.

b) Establishing a framework for cyber security ethics

According to a recent report by Internet and Mobile Association of India (IAMAI), the number of internet users in India has surpassed 500 million by 2018 end. By 2017-year end, India had close to 481 million users, growing by 11.34% from 2016 (Ayyar, 2018). Thus, it is in our best interest to educate and prepare the new workforce.

Majority of the e-commerce users happily prefer the online payment gateways to shop, but the medium of transaction is not always safe. Many prefer Wi-Fi networks which experts always advice to ignore. A safe and secure network should be used for such transactions. Many individuals use harmful websites such as Torrent, Pirate bay etc., and they do not realise that accessing such websites is in complete violation of cyber laws and these websites are best source to plant a virus or a trojan horse in the host system and network which makes it easy for the hackers to conduct malicious activities (Ducklin, 2016). Therefore, it becomes important to establish a literacy agenda on cyber security to educate the citizens through workshops, interactive sessions, documentaries, advertisements, social media campaigns in collaboration with various stakeholders such as cyber security consultancy firms, service providers from banking and finance sectors, various e-commerce entities and business houses to inculcate a habit of safe and secure internet suffering and usage.

c) Ethical hacking is the need of the hour

There is a dire need to identify young and potential hackers and train their unique skills and convert them into the modern-day cyber warriors. The need for ethical hacking can be traced from the fact that every year many Indian firms lose more than $4 billion because of hackers (Jain, 2017). Ethical hacking firms help business houses to safeguard their resources. There are many examples of experts from India who are mastering the field of ethical hacking. Ankit Fadia is a renowned professional hacker who has written over 10 books in computer science and engineering, whereas Rahul Tygai has authored two well acknowledged books on ethical hacking. The future of India lies in the hands of such young cyber warriors.

d) Establishing Regional Cyber Defence Centre (RCDC)

The problem with the current cyber security networks of system is that the entire workload is dependent on the centre. There is no regional cyber defence centre or hub which can intervene and act in the matter of cyber threat or attack. A regional cyber defence centre will act as a governing and monitoring body along with facilitating training and R&D at the regional level. The best possible method which can be adopted is to tie up with various IITs, NITs and ITIs which are located in various states all across India facilitating technical training and education. Establishing regional cyber defence centres in collaboration with these institutions will not only open up various platforms to interact with professionals from the field of cyber security, but will also be an opportunity to initiate a dialogue between various stakeholders. It will even help in monitoring cyber threats and attacks at a very close level and keep a check on any malicious activities originating from that region.

e) Developing National Cyber Security Centre (NCSC)

There seems to be an urgent need to establish a NCSC which will bring out synergy between government bodies and private firms dealing with matters of cyber security. The NCSC will act as a transitional body which will share R&D and facilitate training of individuals.

6.3 Recommendations

a. NCSP should be revised by acknowledging the IT Act 2000. The policy should mention its various aspects of work, including the legality and technicality of the law and how will it be applicable under the policy.

b. The ambiguous nature of the policy should be made more transparent and clearer. The terms and statements mentioned in the policy should be meaningful and should not be left to open interpretation.

c. The policy should formulate a plan of action and a rigid framework which should be implemented to achieve policy objectives.

d. The policy should clearly identify, define and mention various critical information and infrastructure.

e. The policy should acknowledge the role and responsibilities of various organizations and should propose a new structure for better monitoring and surveillance.

f. The policy should address various methods and techniques which will be used for surveillance and data collection methods.

g. The policy should give more details about safeguarding individual privacy with respect to cyber security.

h. The policy should define various roles and responsibilities of 500,000 cyber security professionals and what they are planning to achieve in 5 years, which is a short period of time. According to a study by National Association of Software and Services Companies (NASSCOM), India will need more than 1 million cyber security professionals by 2020 (Narayanan, 2018).

i. The analysis of data from CERT-In Annual reports (2006-11) clearly shows that the level of malicious cyber activities is increasing every year. This can have serious implications on the national security and individual’s privacy. Therefore, there is a great need for a strong policy and an immediate plan of action.

6.4 Conclusion

NCSP is a well thought step but with poor implementation. The policy has also missed out on some important points while aiming for the bigger picture. It needs a dynamic leadership and well-oriented scholars for yielding better results. Therefore, it can be concluded that the proposed hypothesis stands correct. The NCSP 2013 is a holistic approach towards securing Indian Cyberspace. The policy is framed with a coherent vision and a dynamic set of stratagems for execution. But on exposing it to the Indian cyber domain, it is believed to have set high standards which results in several shortcomings in addressing the vulnerabilities of India's Cyberspace.

BIBLIOGRAPHY

1. Abhimanyu, Cyber Security Expert. (2017, September 6). Cyber Security in Schools. *India Today*. Retrieved from https://www.indiatoday.in/education-today/featurephilia/story/cyber-security-in-schools-1037652-2017-09-06/ Accessed on February 15, 2019.
2. Analysis of National Cyber Security Policy (2013) [PDF]. (2013). Retrieved from https://www.dsci.in/sites/default/files/NCSP_2013_DSCI_Analysis_v1.0.pdf/
3. Ayyar, R. (2018, February 20). Number of Indian Internet users will reach 500 million by June 2018 says IAMAI. *The Times of India*. Retrieved from https://timesofindia.indiatimes.com/business/india-business/number-indian-internet-users-will-reach-500-million-by-june-2018-iamai-says/articleshow/62998642.cms/ accessed on February 20, 2019.
4. Bhattacharya, S. (2018, August 2). Kolkata ATM fraud: SIT team to probe card cloning, customers to be refunded. *International Business Times*. Retrieved from https://www.ibtimes.co.in/kolkata-atm-fraud-sit-team-probe-card-cloning-customers-be-refunded-776733/ accessed on March 4, 2019.
5. Burke, J. (2013, September 25). NSA surveillance Indian Embassy UN Mission. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/sep/25/nsa-surveillance-indian-embassy-un-mission/ accessed on March 20, 2019.
6. Captain Chhabra, S. (2014). India's National Cyber Security Policy (NCSP) and Organization – A Critical Assessment [PDF]. Retrieved from https://www.indiannavy.nic.in/sites/default/themes/indiannavy/images/pdf/resources/article_6.pdf/
7. Centre for Internet Security, Cybersecurity Threats. Retrieved from https://www.cisecurity.org/cybersecurity-threats/
8. Christopher, J. (2018, November 1). The Cybersecurity Maturity Model: A Means to Measure and Improve Your Cybersecurity Program. *Forbes*. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/11/01/the-cybersecurity-maturity-model-a-means-to-measure-and-improve-your-cybersecurity-program/#774e2a03680b/ accessed on March 24, 2019.
9. Devi, S., & Rather, M. A. (2015). Cyber Security in India: Problems and Prospects. *IITM Journal of Management and IT, (proceeding of National Conference on Emerging Trends in Information Technology – Cyber Security: A Panoramic View), Volume 6, Issue 1*, p. 59-68.
10. Dilipraj, E., & Reghunadhan. R (2017, June 02). Centre for Air Power Studies (CAPS). *Forum for National Security Studies (FNSS), Volume 47, Issue 17*, p 1-5. Retrieved from http://capsindia.org/files/documents/CAPS_Infocus_DR_24.1.pdf/

11. Ducklin, P. (2016, May 6). Will a visit of the pirate bay end in malware? *Naked Security*. Retrieved from https://nakedsecurity.sophos.com/2016/05/06/will-a-visit-to-the-pirate-bay-end-in-malware/ accessed on February 21, 2019.
12. Fitter, P. M. (2003, February 17). India Cyber Security at Risk. *Business Today*. Retrieved from https://www.businesstoday.in/magazine/features/india-cyber-security-at-risk/story/191786.html/ accessed on February 15, 2019.
13. Ghate, S., & Aggarwal, P. K. (2017). A Literature Review on Cyber Security in Indian Context. *Journal of Computer & Information Technology (JUCIT), Volume 8(5)*, p. 30-36.
14. Goswami, S. (2018, April 6). India's Ministry of Defence Website Defaced. *Data Breach Today*. Retrieved from https://www.databreachtoday.com/indias-ministry-defense-website-defaced-a-10779/ accessed on March 17, 2019.
15. Greenwald, G. & Saxena, S. (2016, June 4). India among top targets of spying by NSA. *The Hindu*. Retrieved from https://www.thehindu.com/news/national/india-among-top-targets-of-spying-by-nsa/article5157526.ece/ accessed on March 20, 2019.
16. Griffith , S. B. (1963). *The Art of War (Translated)*. England: Oxford University Press.
17. Hani, M. N., & Rajan. A. (2018). A Critical Study on Cyber Terrorism with Reference with 26/11 Mumbai Attack. *International Journal of Pure and Applied Mathematics, Volume 119, No. 17*, p. 1617-1636.
18. Howard, R. (2013, December 24). *The Cybersecurity Canon: The Cuckoo's Egg [Blog]*. Retrieved from Paloalto Networks: https://researchcenter.paloaltonetworks.com/2013/12/cybersecurity-canon-cuckoos-egg/ accessed on March 18, 2019.
19. India Today Web Desk. (2018, August 23). 35 percent of attacks on Indian sites are from China: Here are the cyber laws India should know. *India Today.* Retrieved from https://www.indiatoday.in/education-today/gk-current-affairs/story/35-per-cent-of-attacks-on-indian-sites-are-from-china-here-are-the-cyber-laws-that-india-should-know-1321410-2018-08-23/ accessed on March 23, 2019.
20. India's 8 Most Famous Ethical Hackers. Retrieved from https://www.siliconindia.com/news/enterpriseit/Indias-8-Most-Famous-Ethical-Hackers-nid-170533-cid-7.html/ accessed on February 21, 2019.
21. Indian Cyber Security. (2017, August 29). Retrieved from http://www.indiancybersecurity.com/cyber_law/10_salient_features_of_the_information_technology_amendment_act_2008.html/
22. Information and Technology Act 2000, Ministry of Electronics and Information Technology (MeitY), https://meity.gov.in/content/information-technology-act-2000-0/
23. Information and Technology Amendment Act, 2008, Ministry of Electronics and Information Technology (MeitY), http://nagapol.gov.in/PDF/IT%20Act%20(Amendments)2008.pdf/

24. Institute for Defence Studies & Analysis (IDSA). (2012). *India's Cyber Security Challenge*. New Delhi: IDSA Task Force Report.
25. International Telecommunication Union (ITU). (2017). *Global Cybersecurity Index (GCI)*, Geneva, Switzerland: ITU. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf/
26. Jain, V. (2017, September 18). Ethical Hacking. *India Today*. Retrieved from https://www.indiatoday.in/education-today/jobs-and-careers/story/ethical-hacking-1047211-2017-09-18/ accessed on February 21, 2019.
27. Java Point, History of Cyber Security. Retrieved from https://www.javatpoint.com/history-of-cyber-security/
28. Kaspersky Resource Centre, Cyber Security. Retrieved from https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security/
29. Kaul, S. (2019, March 24). Virtual SIMs used in Pulwama terror attack; India to approach US for help. *Press Trust of India (PIT)*. Retrieved from https://repository.inshorts.com/articles/en/PTI/c29e050a-381a-44f7-a849-8675ca8cd3ec?utm_campaign=fullarticle&utm_medium=referral&utm_source=inshorts/ accessed on March 25, 2019
30. Kaushik, M. (2003, February 17). India Cyber Security at Risk. *Business Today.* Retrieved from https://www.businesstoday.in/magazine/features/india-cyber-security-at-risk/story/191786.html/ accessed on February 15, 2019
31. Kharia, R., Sethi, A., & Sathe, G. (2018, November 11). UIDAI's Aadhaar Software hacked ID database compromised Experts Confirm. *Huffington Post*. Retrieved from https://www.huffingtonpost.in/2018/09/11/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_a_23522472/ accessed on March 24, 2019.
32. Kizza, J M. (2005), *Guide to Computer Network Security*, 3rd Edition, Springer. Retrieved from http://www.myjetking.com/wp-content/uploads/2015/11/Guide-to-Computer-Network-Security-3rd-Edition-2015.pdf/
33. m@dhu. (2012, April 12). Networks (ERNET, NICNET, OCLC, INFLIBNET, DELNET, JANET, BLAISE) [Blog post]. Retrieved from http://netjrflibraryandinformationscience.blogspot.com/2012/04/unit-viii-networks-ernet-nicnet-oclc.html/ accessed on March 15, 2019.
34. Maj Gen Mallick, P. K. (2017). Cyber Security in India: Present Status. *Vivekananda International Foundation, Issue Brief.*
35. Ministry of Electronics & Information Technology (MeitY), CERT-In Annual Report 2006-17.
36. Ministry of External Affairs, Media Centre, "India-US Cyber Security Forum – Fact Sheet" (2006, March 2) https://www.mea.gov.in/bilateral-documents.htm?dtl/6014/IndiaUS+Cyber+Security+Forum++Fact+Sheet/ accessed on March 20, 2019.
37. Mishra, S., Dhir, S., & Hooda, M., (2016). A Study on Cyber Security, Its Issues and Cyber Crime Rates in India. *Innovations in Computer Science and Engineering,*

(proceeding of International Conference on Innovations in Computer Science & Engineering (ICICSE 2015)) p. 249-253.

38. Naik, S. (2017). A Biggest Threat to India – Cyber Terrorism and Crime. *Journal of Research in Humanities and Social Science, Volume 5, Issue 4*, p. 27-30.
39. Narayanan, A. (2018, July 2). Top 5 Cyber security jobs growing demand in India. *CSO Online*. Retrieved from https://www.csoonline.in/opinion/top-5-cyber-security-jobs-growing-demand-india/ accessed on March 25, 2019.
40. National Critical Information Infrastructure Protection Centre (NCIIPC), About us, http://nciipc.gov.in/
41. National Cyber Security Policy (NCSP) – 2013, Ministry of Electronics and Information Technology (MeitY), Preamble, 1, page no 2.
42. Pathak, A., & Sharma, R. (2015). Cybercrime and Information Warfare – The New Arena of War. *IITM Journal of Management and IT, (proceeding of National Conference on Emerging Trends in Information Technology – Cyber Security: A Panoramic View), Volume 6, Issue 1*, p. 129-134.
43. Peter, P. (2017, August 27). Many Bengalureans lose cash to sim card swap fraud. *The Times of India.* Retrieved from https://timesofindia.indiatimes.com/city/bengaluru/many-bengalureans-lose-cash-to-sim-card-swap-fraud/articleshow/58387867.cms/ accessed by March 10, 2019.
44. Press Trust of India (PTI). (2008, April 27). Defacement of Indian Website on Rise. *The Economic Times*. Retrieved from https://economictimes.indiatimes.com/tech/internet/defacement-of-indian-website-on-rise/articleshow/2988200.cms/ accessed on March 17, 2019.
45. Press Trust of India (PTI). (2018, August 14). Cosmos Bank's server hacked; Rs 94 crore siphoned off in 2 days. *The Economic Times*. Retrieved from https://economictimes.indiatimes.com/industry/banking/finance/banking/cosmos-banks-server-hacked-rs-94-crore-siphoned-off-in-2-days/articleshow/65399477.cms/ accessed on March 4, 2018.
46. Press Trust of India (PTI). (2018, May 13). India needs 3 million cyber security professionals right now – IBM. *Business Standards*. Retrieved from https://www.business-standard.com/article/companies/india-needs-3-million-cyber-security-professionals-right-now-ibm-118051300153_1.html/ accessed on March 24, 2019.
47. Press Trust of India (PTI). (2018, November 12). India witnessed over 6.95 lakh Cyber Attacks from Russia, U.S., others. *Bloomberg Quint.* Retrieved from https://www.bloombergquint.com/business/india-witnesses-over-4-36-lakh-cyberattacks-from-russia-us-others-in-jan-jun-f-secure#gs.TFHBmuXl/ accessed on March 26, 2019.
48. Purushottam, S. (2018, October 27). Chinese threat to Cyber Security: Why India needs a comprehensive & concrete action plan for national security and economic health. *Financial Express*. Retrieved from https://www.financialexpress.com/opinion/chinese-threat-to-cybersecurity-

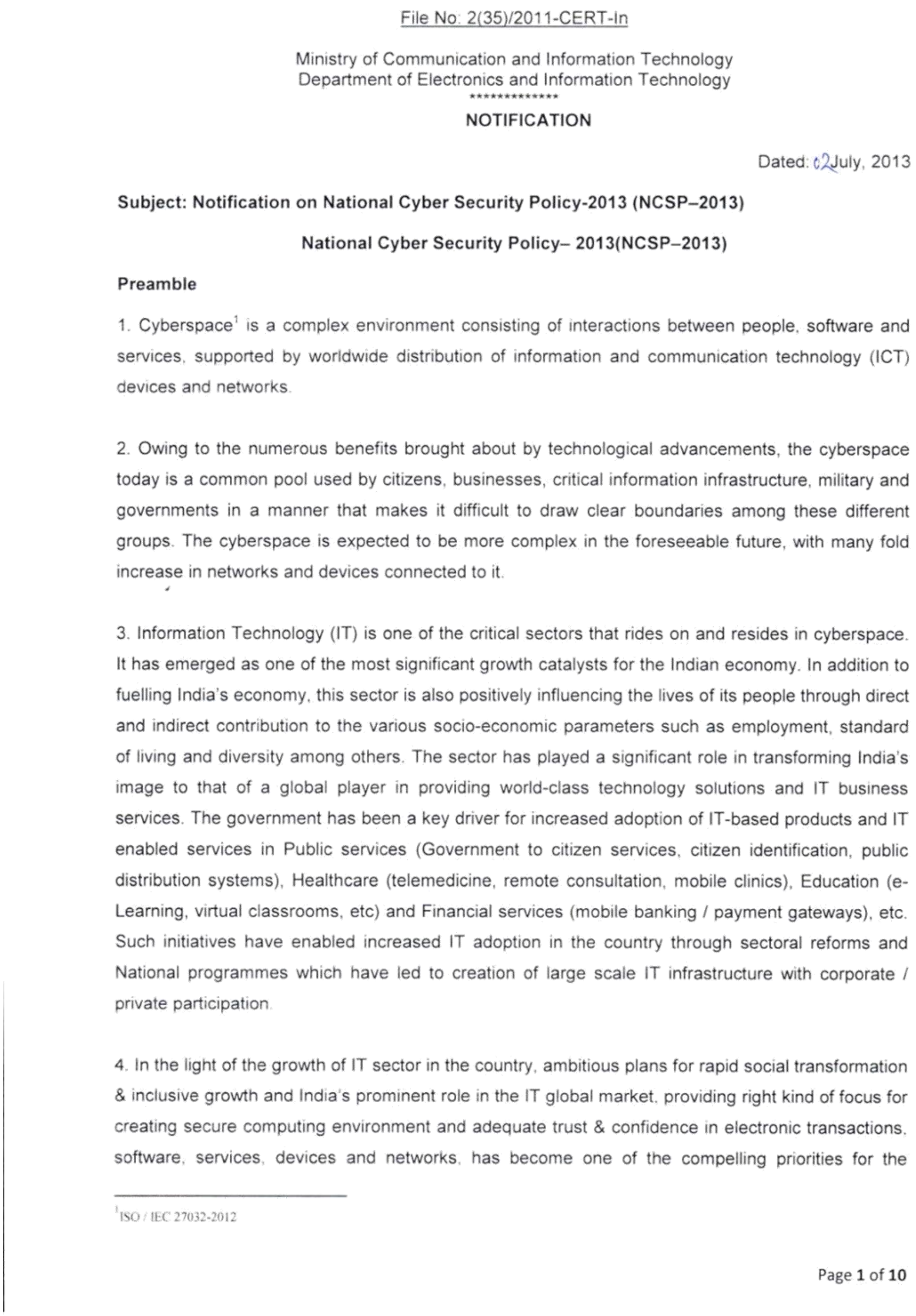
why-india-needs-a-comprehensive-concrete-action-plan-for-national-security-and-economic-health/1363012/ accessed on March 24, 2019.

49. Raytheon, The Wisdom of "Wargames". Retrieved from https://www.raytheon.com/cyber/news/feature/wisdom-wargames/
50. Rossow, A. Internet Attorney. (2018, February 28). Cyberbullying taken to a whole new level, enter the blue whale challenge. *Forbes*. Retrieved from https://www.forbes.com/sites/andrewrossow/2018/02/28/cyberbullying-taken-to-a-whole-new-level-enter-the-blue-whale-challenge/#536117f42673/ accessed on February 17, 2019.
51. Samuel, C. & Sharma, M. (2016). *Securing Cyberspace: International and Asian perspectives*, Institute for Defence Studies & Analysis (IDSA), New Delhi.
52. Sharma, A. (2013, November 8). Indian Cyber Security has loopholes. *The New Indian Express*. Retrieved from http://www.newindianexpress.com/cities/hyderabad/2013/nov/08/Indian-cyber-security-has-loopholes-535085.html/ accessed on March 26, 2019.
53. Sharma, K., & Bhalla, T. (2015). Future Towards Danger: The Terror of Cyber Attacks. *IITM Journal of Management and IT, (proceeding of National Conference on Emerging Trends in Information Technology – Cyber Security: A Panoramic View), Volume 6, Issue 1,* p. 90-94.
54. Significant Cyber Incidents Since 2006, Centre for Strategic and International Studies (CSIS), 2017. Available online at https://www.csis.org/programs/technology-policy-program/cybersecurity/other-projects-cybersecurity/significant-cyber/ accessed on March 26, 2019.
55. Singh, B. P., & Verma, A. (2015). Cyber Terrorism – An International Phenomena and an Eminent Threat. *IITM Journal of Management and IT, (proceeding of National Conference on Emerging Trends in Information Technology – Cyber Security: A Panoramic View), Volume 6, Issue 1,* p. 164-168.
56. Singh, N., & Rishi, A. (2015). Pyramid: A case study of Cyber Security in India. *South Asian Journal of Business and Management Cases 4(I)*, p. 135-142.
57. Singh, O., Gupta, P., & Kumar, R. (2016). A Review of Indian Approach towards Cybersecurity. *International Journal of Current Engineering and Technology, Vol.6, No.2*, p. 644-648.
58. Singh, R. K. (2015). Nine Steps to Indian Security, Confidentiality, Privacy & Technology in Cyber Space. *IITM Journal of Management and IT, (proceeding of National Conference on Emerging Trends in Information Technology – Cyber Security: A Panoramic View), Volume 6, Issue 1,* p. 12-16.
59. Singh, V. (2013, August 26). Point out the function of National Information Board in Cyber Security. Retrieved from http://www.preservearticles.com/2012032027854/point-out-the-function-of-national-information-board-in-cyber-security.html/ accessed on March 15, 2019.
60. The Hans India. (2016, December 6). An Overview on Cyber Security Policy in India. *The Hans India*. Retrieved from

https://www.thehansindia.com/posts/index/Hans/2016-12-09/An-overview-on-cyber-security-policy-in-India/267807/ accessed on March 25, 2019.

61. Tonje, A. M., Kasture, S. S., & Chaudhari, S. R. (2013). Cyber Security: Challenges for society – Literature Review. *IOSR Journal of Computer Engineering (IOSR-JCE), Volume 12, Issue 2*, p. 67-75.
62. Verma, A. K., & Sharma, A. K. (2014). Cyber Security Issues and Recommendations. *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 4,* p. 629-634.

APPENDIX A: NATIONAL CYBER SECURITY POLICY (NCSP) 2013



File No: 2(35)/2011-CERT-In

Ministry of Communication and Information Technology
Department of Electronics and Information Technology
****

NOTIFICATION

Dated: 02July, 2013

Subject: Notification on National Cyber Security Policy-2013 (NCSP–2013)

National Cyber Security Policy– 2013(NCSP–2013)

Preamble

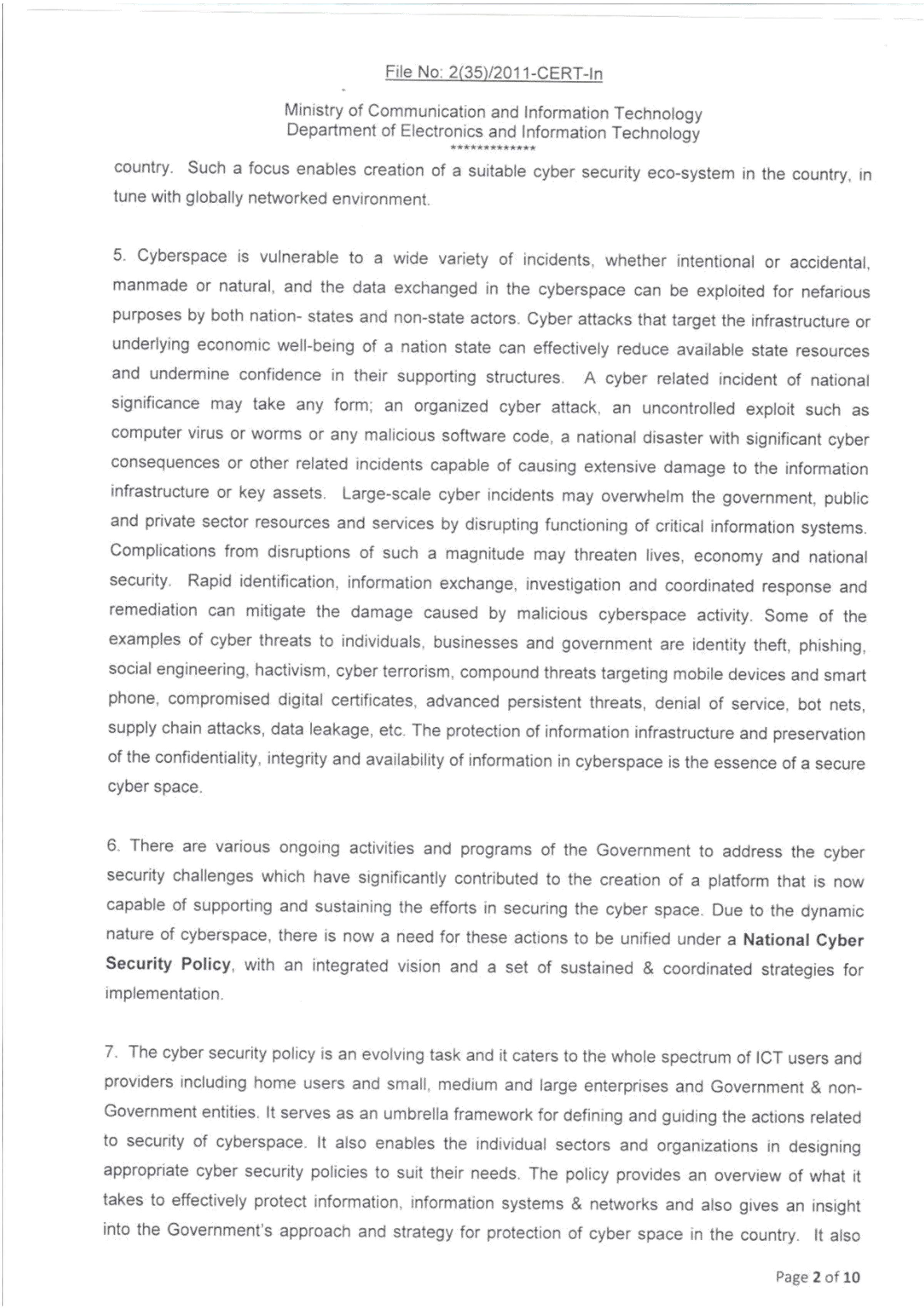
1. Cyberspace[1] is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technology (ICT) devices and networks.

2. Owing to 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.

3. 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. The government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (Government to citizen services, citizen identification, public distribution systems), Healthcare (telemedicine, remote consultation, mobile clinics), Education (e-Learning, virtual classrooms, etc) and Financial services (mobile banking / payment gateways), etc. Such initiatives have enabled increased IT adoption in the country through sectoral reforms and National programmes which have led to creation of large scale IT infrastructure with corporate / private participation.

4. 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

[1] ISO / IEC 27032-2012

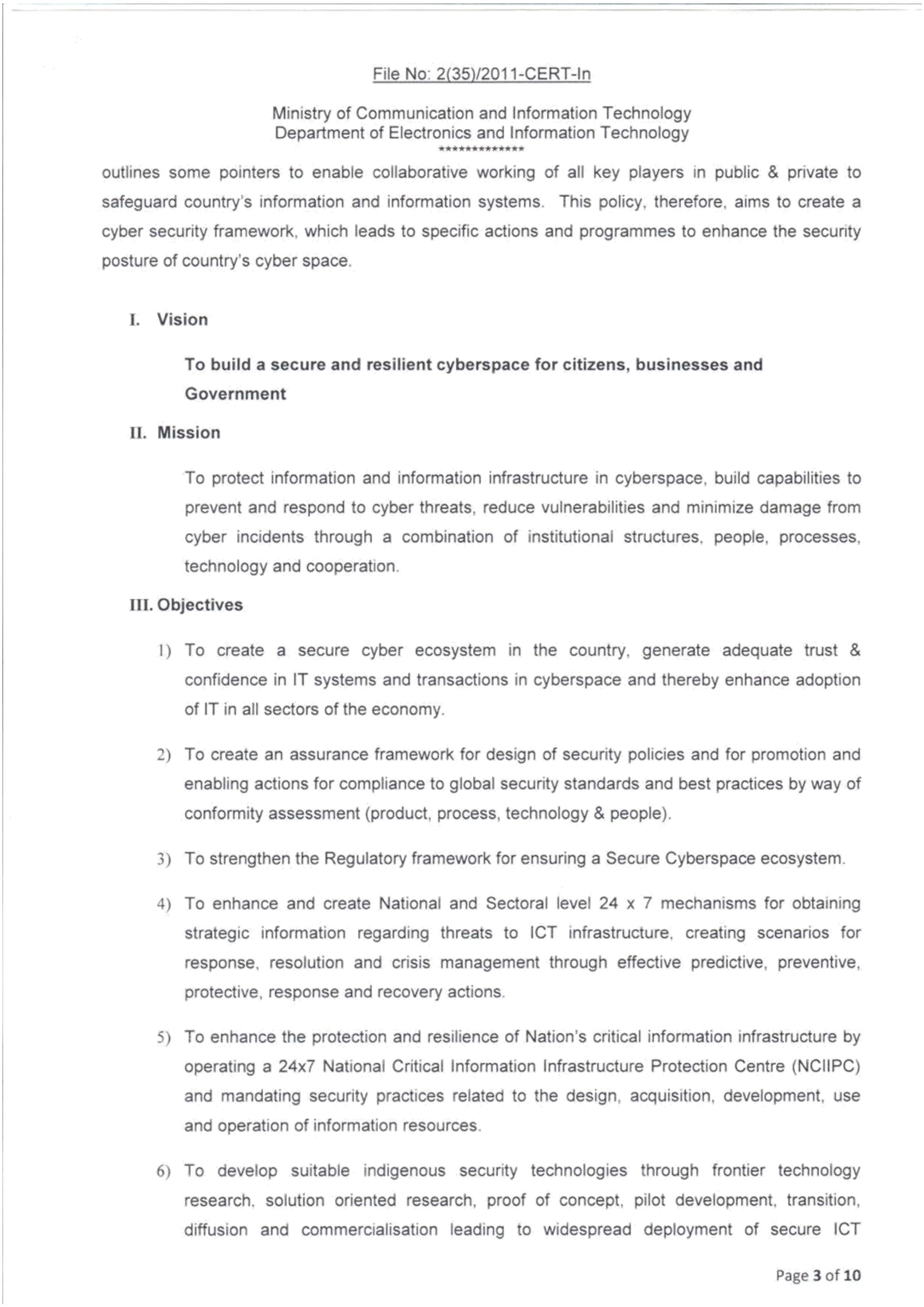


country. Such a focus enables creation of a suitable cyber security eco-system in the country, in tune with globally networked environment.

5. Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation- states and non-state actors. 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. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, hactivism, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

6. 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 under a **National Cyber Security Policy**, with an integrated vision and a set of sustained & coordinated strategies for implementation.

7. 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 serves as an umbrella framework for defining and guiding the actions related to security of cyberspace. It also 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. 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.

I. Vision

To build a secure and resilient cyberspace for citizens, businesses and Government

II. Mission

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.

III. Objectives

1) 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.

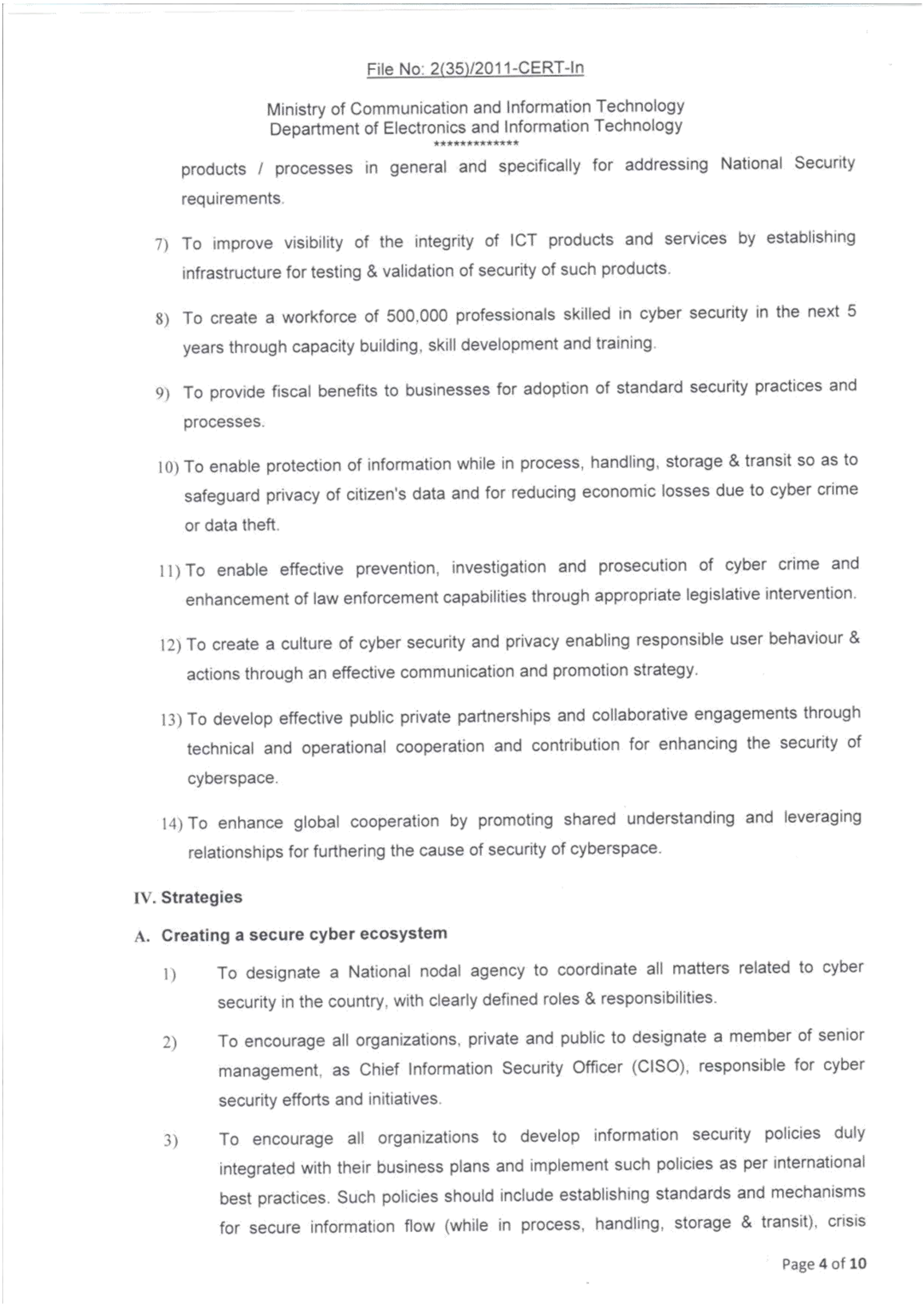
2) To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).

3) To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem.

4) To enhance and create National and Sectoral 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.

5) 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.

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 the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products.

8) To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.

9) To provide fiscal benefits to businesses for adoption of standard security practices and processes.

10) To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft.

11) To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.

12) To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.

13) To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.

14) To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.

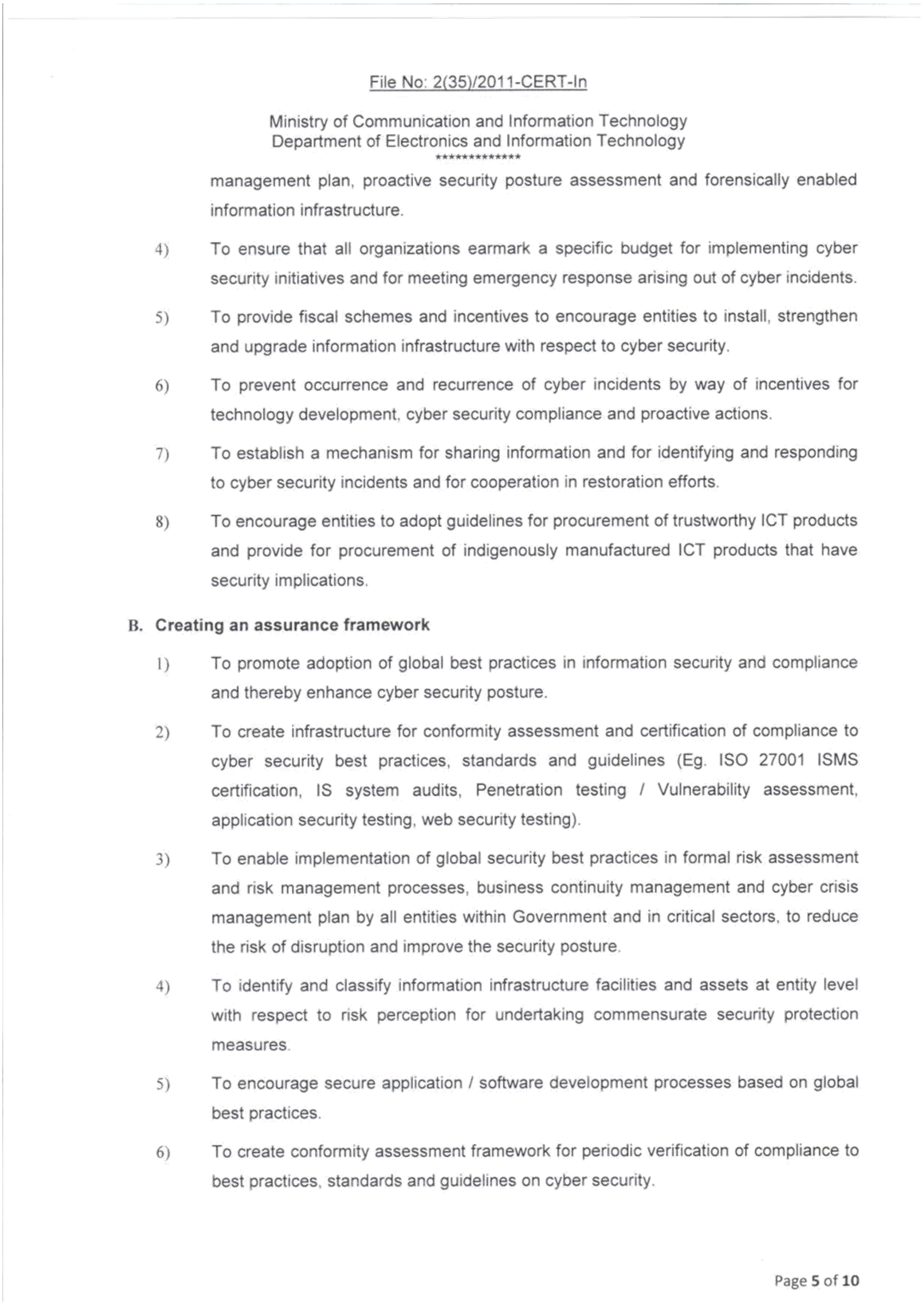
IV. Strategies

A. Creating a secure cyber ecosystem

1) To designate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.

2) To encourage all organizations, private and public to designate a member of senior management, as Chief Information Security Officer (CISO), responsible for cyber security efforts and initiatives.

3) To encourage all organizations to develop information security policies duly integrated with their business plans and implement such policies as per international best practices. Such policies should include establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis



management plan, proactive security posture assessment and forensically enabled information infrastructure.

4) To ensure that all organizations earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.

5) To provide fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security.

6) To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions.

7) To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.

8) To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implications.

B. Creating an assurance framework

1) To promote adoption of global best practices in information security and compliance and thereby enhance cyber security posture.

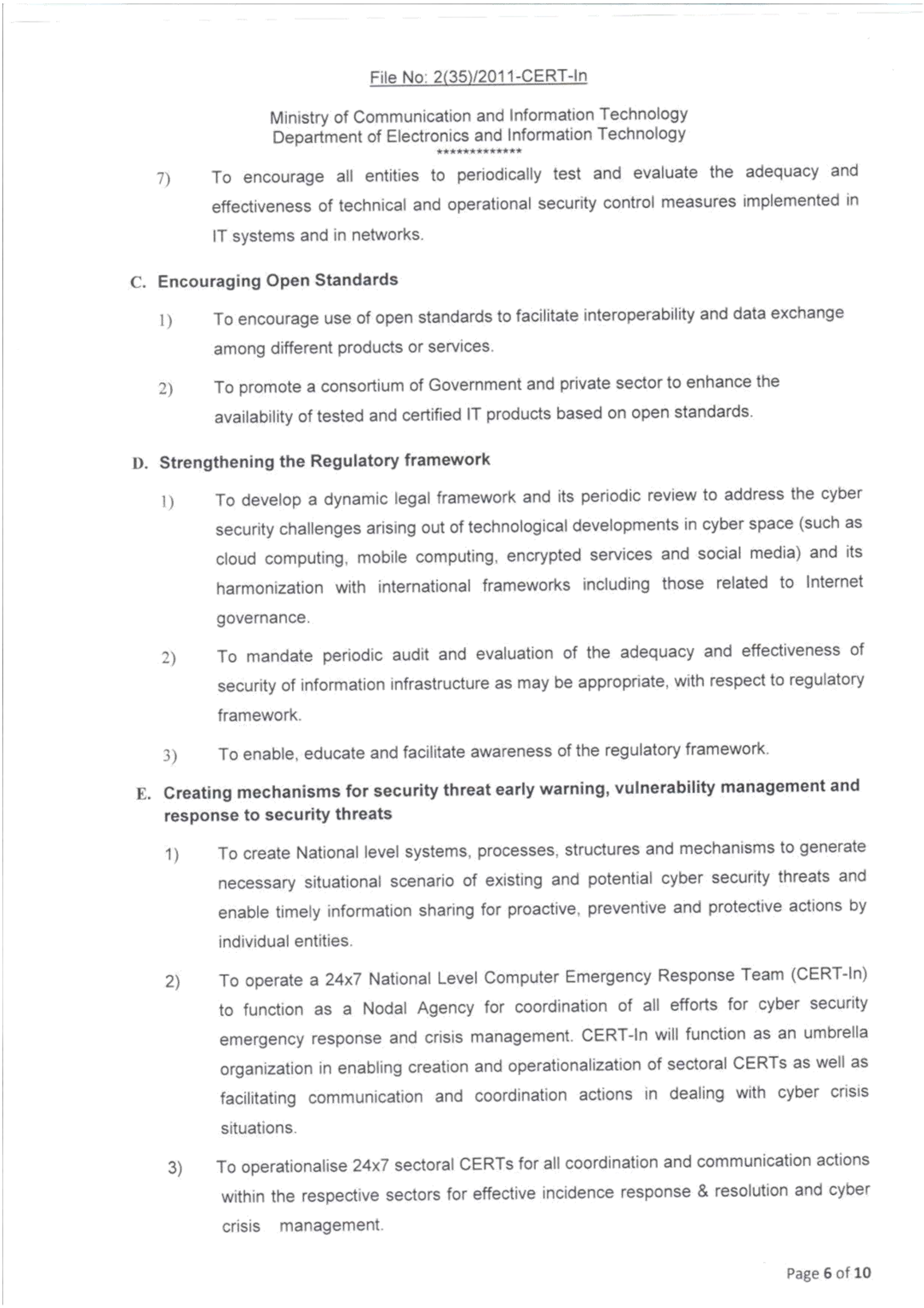
2) To create infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines (Eg. ISO 27001 ISMS certification, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing).

3) To enable implementation of global security best practices in formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all entities within Government and in critical sectors, to reduce the risk of disruption and improve the security posture.

4) To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.

5) To encourage secure application / software development processes based on global best practices.

6) To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security.



7) To encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and in networks.

C. Encouraging Open Standards

1) To encourage use of open standards to facilitate interoperability and data exchange among different products or services.

2) To promote a consortium of Government and private sector to enhance the availability of tested and certified IT products based on open standards.

D. Strengthening the Regulatory framework

1) To develop a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space (such as cloud computing, mobile computing, encrypted services and social media) and its harmonization with international frameworks including those related to Internet governance.

2) To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate, with respect to regulatory framework.

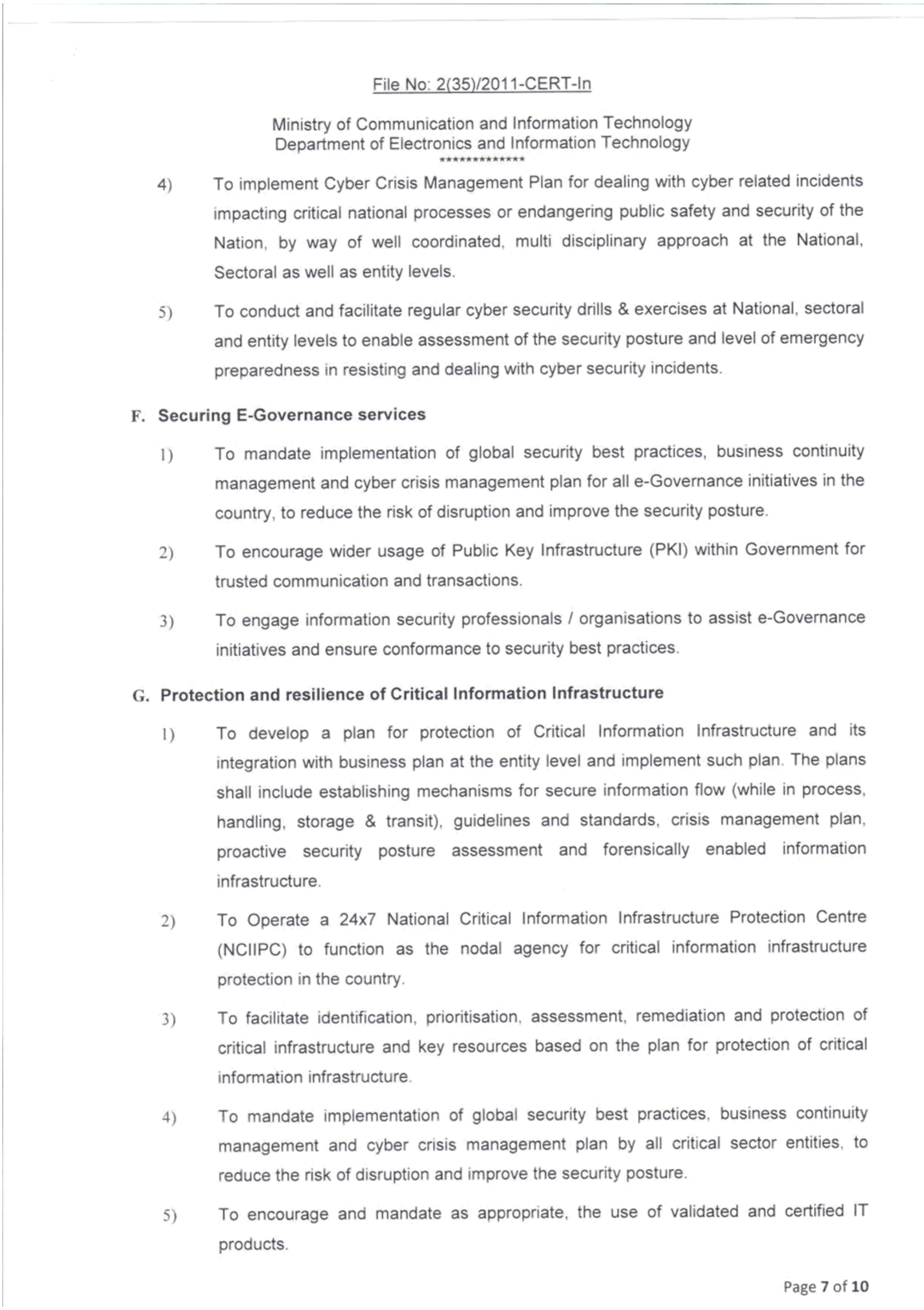
3) To enable, educate and facilitate awareness of the regulatory framework.

E. Creating mechanisms for security threat early warning, vulnerability management and response to security threats

1) To create National level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

2) To operate a 24x7 National Level Computer Emergency Response Team (CERT-In) to function as a Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management. CERT-In will function as an umbrella organization in enabling creation and operationalization of sectoral CERTs as well as facilitating communication and coordination actions in dealing with cyber crisis situations.

3) To operationalise 24x7 sectoral CERTs for all coordination and communication actions within the respective sectors for effective incidence response & resolution and cyber crisis management.



4) To implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical national processes or endangering public safety and security of the Nation, by way of well coordinated, multi disciplinary approach at the National, Sectoral as well as entity levels.

5) To conduct and facilitate regular cyber security drills & exercises at National, sectoral and entity levels to enable assessment of the security posture and level of emergency preparedness in resisting and dealing with cyber security incidents.

F. Securing E-Governance services

1) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the country, to reduce the risk of disruption and improve the security posture.

2) To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.

3) To engage information security professionals / organisations to assist e-Governance initiatives and ensure conformance to security best practices.

G. Protection and resilience of Critical Information Infrastructure

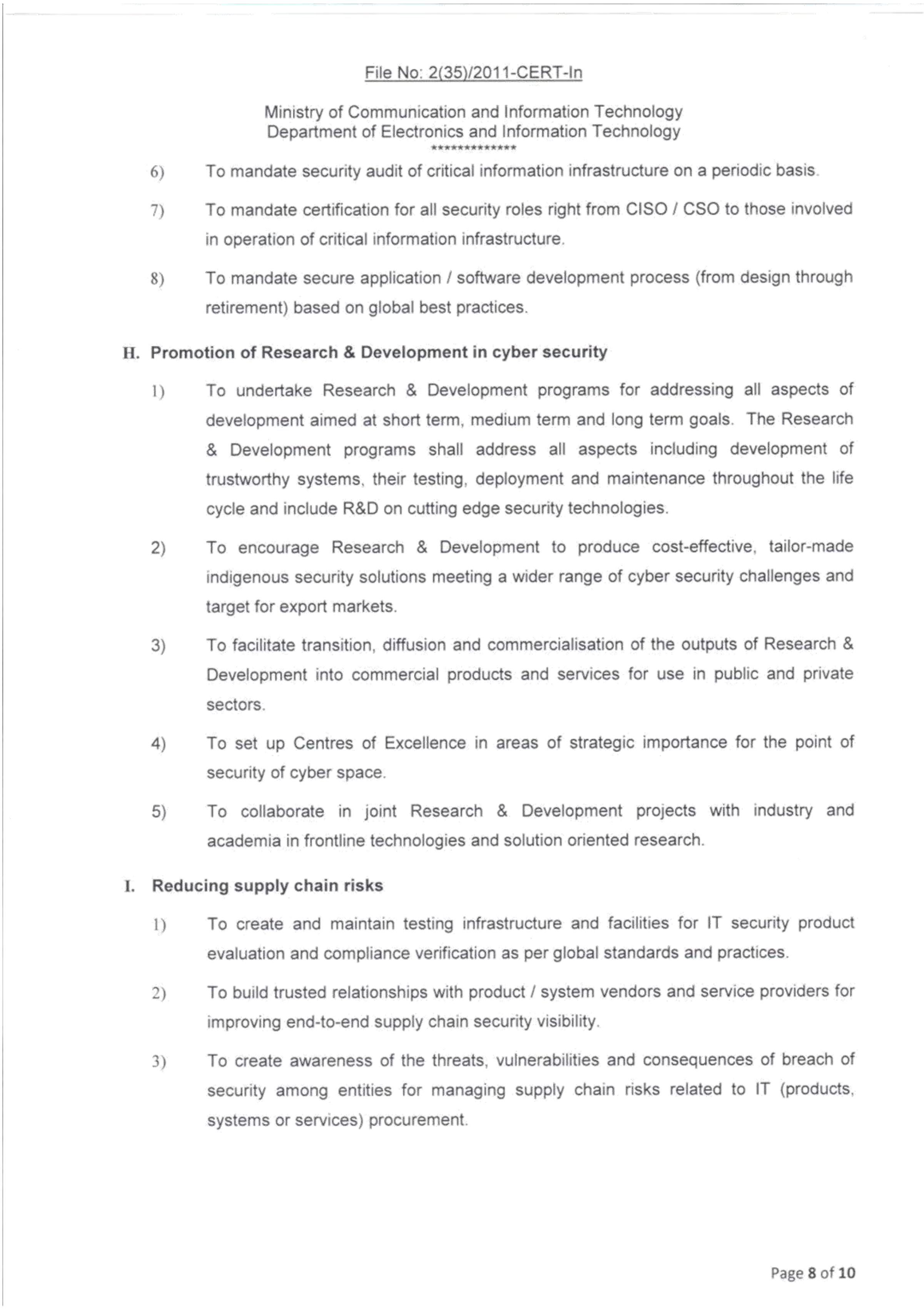
1) To develop a plan for protection of Critical Information Infrastructure and its integration with business plan at the entity level and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

2) To Operate a 24x7 National Critical Information Infrastructure Protection Centre (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country.

3) To facilitate identification, prioritisation, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure.

4) To mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all critical sector entities, to reduce the risk of disruption and improve the security posture.

5) To encourage and mandate as appropriate, the use of validated and certified IT products.



6) To mandate security audit of critical information infrastructure on a periodic basis.

7) To mandate certification for all security roles right from CISO / CSO to those involved in operation of critical information infrastructure.

8) To mandate secure application / software development process (from design through retirement) based on global best practices.

H. Promotion of Research & Development in cyber security

1) To undertake Research & Development programs for addressing all aspects of development aimed at short term, medium term and long term goals. The Research & Development programs shall address all aspects including development of trustworthy systems, their testing, deployment and maintenance throughout the life cycle and include R&D on cutting edge security technologies.

2) To encourage Research & Development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets.

3) To facilitate transition, diffusion and commercialisation of the outputs of Research & Development into commercial products and services for use in public and private sectors.

4) To set up Centres of Excellence in areas of strategic importance for the point of security of cyber space.

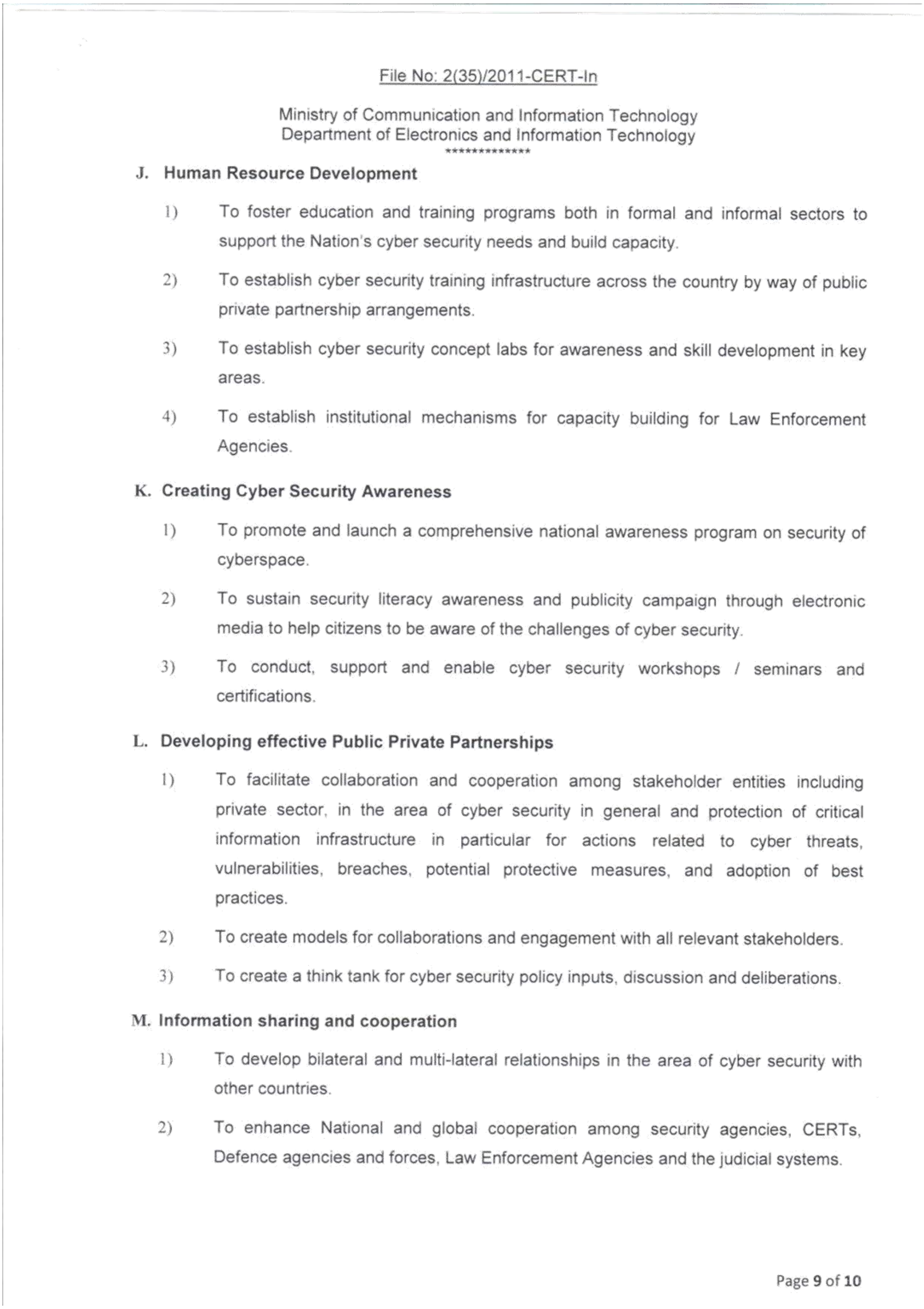
5) To collaborate in joint Research & Development projects with industry and academia in frontline technologies and solution oriented research.

I. Reducing supply chain risks

1) To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices.

2) To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility.

3) To create awareness of the threats, vulnerabilities and consequences of breach of security among entities for managing supply chain risks related to IT (products, systems or services) procurement.



File No: 2(35)/2011-CERT-In

Ministry of Communication and Information Technology
Department of Electronics and Information Technology
****

J. Human Resource Development

1) To foster education and training programs both in formal and informal sectors to support the Nation's cyber security needs and build capacity.

2) To establish cyber security training infrastructure across the country by way of public private partnership arrangements.

3) To establish cyber security concept labs for awareness and skill development in key areas.

4) To establish institutional mechanisms for capacity building for Law Enforcement Agencies.

K. Creating Cyber Security Awareness

1) To promote and launch a comprehensive national awareness program on security of cyberspace.

2) To sustain security literacy awareness and publicity campaign through electronic media to help citizens to be aware of the challenges of cyber security.

3) To conduct, support and enable cyber security workshops / seminars and certifications.

L. Developing effective Public Private Partnerships

1) 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.

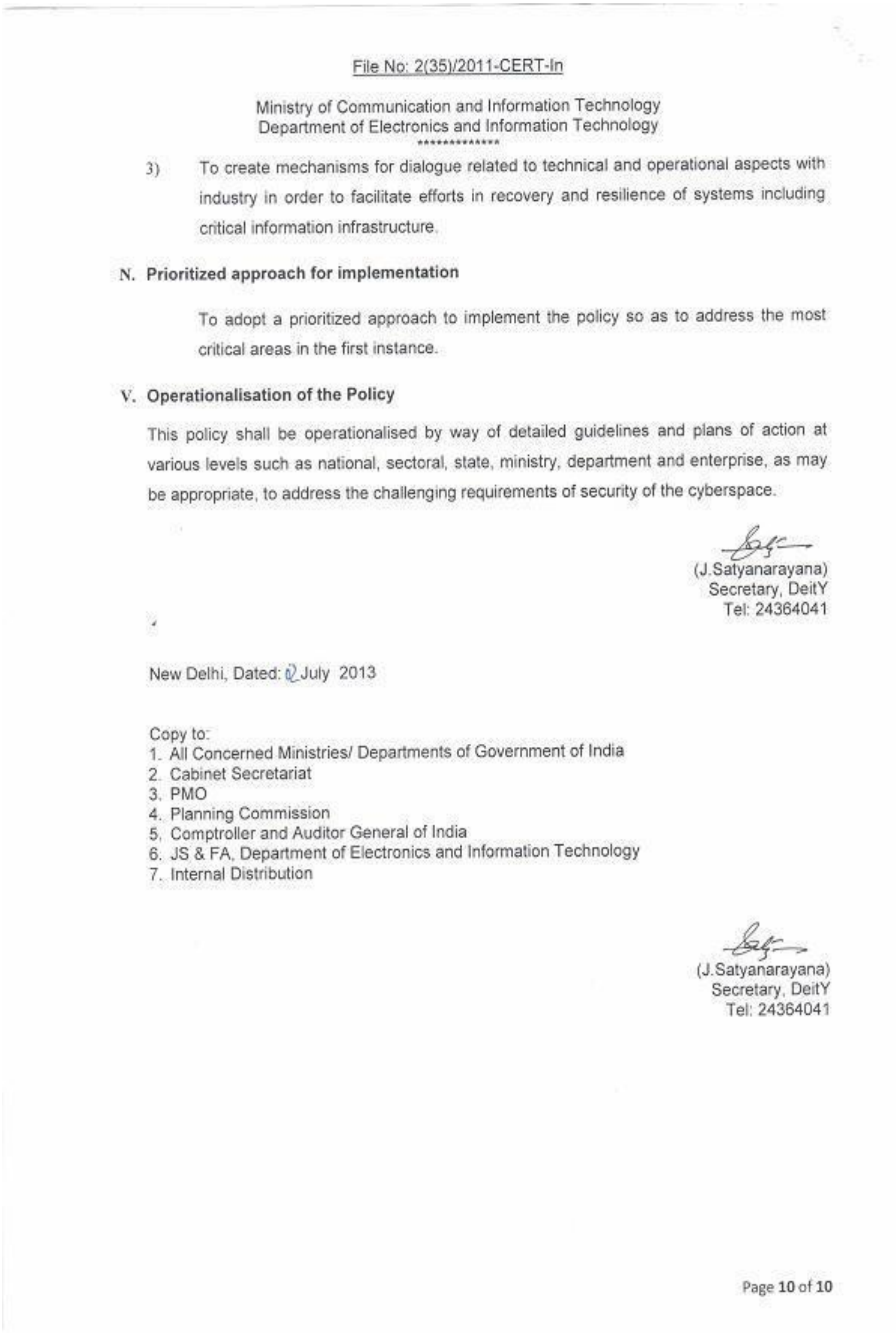
2) To create models for collaborations and engagement with all relevant stakeholders.

3) To create a think tank for cyber security policy inputs, discussion and deliberations.

M. Information sharing and cooperation

1) To develop bilateral and multi-lateral relationships in the area of cyber security with other countries.

2) To enhance National and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement Agencies and the judicial systems.



File No: 2(35)/2011-CERT-In

Ministry of Communication and Information Technology
Department of Electronics and Information Technology
****

3) To create mechanisms for dialogue related to technical and operational aspects with industry in order to facilitate efforts in recovery and resilience of systems including critical information infrastructure.

N. Prioritized approach for implementation

To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.

V. Operationalisation of the Policy

This policy shall be operationalised by way of detailed guidelines and plans of action at various levels such as national, sectoral, state, ministry, department and enterprise, as may be appropriate, to address the challenging requirements of security of the cyberspace.

(J.Satyanarayana)
Secretary, DeitY
Tel: 24364041

New Delhi, Dated: 2 July 2013

Copy to:
1. All Concerned Ministries/ Departments of Government of India
2. Cabinet Secretariat
3. PMO
4. Planning Commission
5. Comptroller and Auditor General of India
6. JS & FA, Department of Electronics and Information Technology
7. Internal Distribution

(J.Satyanarayana)
Secretary, DeitY
Tel: 24364041

APPENDIX B: GLOSSARY

Types of Cyber Attacks		
No.	**Term(s)**	**Definition(s)**
1.	**Bluetooth Hijacking (Bluejacking)**	It is kind of attack where devices with Bluetooth connectivity are targeted. Mobile phones, Personal Digital Assistance (PDA) and laptops are the best examples.
2.	**Browser Hijacking**	It refers to a malicious software which unintendingly changes the settings of the web browser using admin authorization. These changes can be harmful in nature since the software can allow any virus, worm, spyware and malware to install itself in the system and exploit the user's data and information.
3.	**Denials of Service (DoS)**	As the name itself suggest 'denial of service' which means a temporary or permanent stoppage of the service. The attack prevents the authorized users from accessing the computer and other devices connected to it including the network. The attack overwhelms the users since their network is flooded with traffic which it is impossible for them to access it.
4.	**Distributed denial-of-Service (DDoS)**	It is similar DoS. The attack attempts to disrupt the normal follow of traffic on the sever or a network and try to flood it with unusual traffic. In simple words, it like a traffic jam blocking the road and preventing the smooth flow of traffic.
5.	**E-Mail Related Crimes**	These sorts of cyber-crimes are very common now-a-days. It is one of the simplest ways to infect a standalone computer or a network with any harmful virus or worm. The perpetrator attaches a virus or a worm in a mail and send it across various networks. As soon as the individuals clicks on the attached file, the virus activates and infect the entire system.
6.	**Hacking**	It a malicious practice of accessing a computer or a network without any authorization from the users or the admin. The person responsible for hacking is known as a hacker.

7.	**Logic Bomb**	A logic bomb seems to be a fine working useful software which contain a malicious hidden code which when activated can destroy sensitive data, information, computer drives, application and other software.
8.	**Identity Theft**	Identity Theft refers to stealing individual's personal information with an intent use that information in a corrupt or deceiving manner.
9.	**Keyboard Logging**	It is a form of surveillance system which once installed in any computer records every keystroke typed on a specific (physical) keyboard. The keystrokes recorded are stored in form of a log which is usually encrypted.
10.	**Malware**	Malware is also known as malicious software is any form of program or file which when installed on a computer have the potential to destroy, harm or manipulate any data or information. It is usually installed with a motif of compromising the secrecy, veracity and accessibility of the user's information.
11.	**Pharming**	It is another popular cyber-attack used by hackers. In such sort of attacks, the users are directed into to illegitimate, fake or false website pretending to be an authentic one and steal the individual's data or personal information.
12.	**Phishing**	It is a kind of cybercrime where perpetrators personify themselves as a legitimate individual from an institution or organization and lure users to reveal their personal information such a password, bank account details and credit card numbers. Such type of attacks is directed with the help of text messages, phone calls and emails.
13.	**Ransomware**	It can be classified as a malware which averts or restricts the individual from gaining access to their computers, either by locking the computer's screen or by locking the individual's file unless and until a ransom is paid to the hacker.

14.	**Spamming**	It is defined as the use of electronic messaging system such as email to send unwanted bulk messages to many people at the same. It means that sending an email, to large chunk of people who have not registered for the subscription. The email is a generally in form of an advertisement.
15.	**Spoofing**	It is a form of an attack where the perpetrator pretends to be the user itself and tries to gain unauthorised access to the user's computer to steal in some personal information such as credentials and password.
16.	**Spyware**	It is a form of malware which is secretly installed in the individual's computer and damage the utilities of the system as well as the network without the knowledge of the individual. Such type of an attack can has various motives behind it such as identity theft, stealing of data and information such as bank account details, credit card details, internet data usage and much more.
17.	**Trojans/ Trojan horse**	It is a form of malware code or computer program which looks like a legitimate software but is completely malicious in nature. It acts as an authentic computer application in order to trick the user. A trojan usually deceive it's users by installing and executing malware or virus into the system. Once a trojan is launched, it will perform its necessary functions for which it was created. Its main function is to steal, damage, destroy or temporarily disable the computer services.
18.	**Virus**	It is a type of illegitimate code or a program created in order to avert, prevent or manipulate the method in which the system or a computer operates. The speciality about virus is that it designed to spread across various computers and networks. The virus has an equal potential to disrupt, corrupt, damage or destroy the system data.
19.	**Worm(s)**	Worm is a type of malware which replicates itself without any human intervention and spread across like a virus from computer to computer. The interesting fact about worm is that it does not need to attach itself to a program file unlike virus and other malware but the intensity of the damage still remains the same.
20.	**Zero-day Vulnerability**	A zero-day vulnerability is a serious cyber security concern. It is a flaw in the computer software known only to the vendor until a fix is available in the market. Such a flaw leaves the user vulnerable to any form of cyber-attack from the hackers which have the potential to exploit it.

Ever since the events of document leaks by NSA's whistle blower Edward Snowden, countries around the world have become conscious about their cyber security measures. The leaked reports worked as a wake-up call for India. India was the top most priority target by American spy agency NSA. It was time when India realized the great need of Cyber Policy. In the year 2013, Ministry of Electronics and Information Technology (MeitY) drafted India's first National Cyber Security Policy (NCSP). The policy is framed with a coherent vision and a dynamic set of stratagems for execution. It is aimed at building a secure and resilient cyber space for its citizens, businesses and government. It is considered to be a dynamic step in building the foundation of new India. The newly formulated policy is a holistic approach towards securing Indian Cyberspace. But over the years, it does not seem to be effective enough to safeguard the Indian Cyberspace. The implementation of the policy is poorly executed. Since the time, the policy was made public. It had been in the limelight for criticism by various scholars and organizations. As complex it defines the cyberspace, it stands out to be of the similar nature. This Monograph is aimed at understanding the NCSP and its implications. It identifies various shortcomings of the policy. It also analyses data related to cyber security incidents in India gathered from CERT-In Annual reports of 11 years (2006-17). After the brief analysis of policy and data, the study made some valuable inputs in the form of recommendations for the revision of NCSP and strive towards building a secure cyberspace.

Saurabh Singh is an alumnus of Symbiosis School of International Studies, Pune where he completed his Masters in International Studies. He is a graduate in English Language and Literature from Christ College, Rajkot. He was a former research and policy intern at Brookings India. He is a keen learner and policy enthusiast. Policy matters and subjects such as Cyber Security, Digital Diplomacy, India's Foreign Policy & National Security, Indo-Pacific, Climate Change & Energy Security, and India's role in the changing world order are his key areas of research interest.