52

**STANDING COMMITTEE ON**

**INFORMATION TECHNOLOGY**

**(2013-14)**

**FIFTEENTH LOK SABHA**

**MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY**

**(DEPARTMENT OF ELECTRONICS AND INFORMATION TECHNOLOGY)**

# CYBER CRIME, CYBER SECURITY AND RIGHT TO PRIVACY

**FIFTY-SECOND REPORT**


**LOK SABHA SECRETARIAT**

**NEW DELHI**

***February, 2014/Magha, 1935 (Saka)***

**FIFTY-SECOND REPORT**

**STANDING COMMITTEE ON**

**INFORMATION TECHNOLOGY**

**(2013-14)**

**(FIFTEENTH LOK SABHA)**

# MINISTRY OF COMMUNICATIONS AND INFORMATION TECHNOLOGY
# (DEPARTMENT OF ELECTRONICS AND INFORMATION TECHNOLOGY)

# CYBER CRIME, CYBER SECURITY AND RIGHT TO PRIVACY

**FIFTY SECOND REPORT**

***Presented to Lok Sabha on 12th February, 2014***

***Laid in Rajya Sabha on 12th February, 2014***


**LOK SABHA SECRETARIAT**

**NEW DELHI**

***February, 2014/ Magha, 1935 (Saka)***

**CONTENTS**

**COMPOSITION OF THE STANDING COMMITTEE ON INFORMATION TECHNOLOGY (2013-14)**

**Shri Rao Inderjit Singh - Chairman**

**Lok Sabha**

2. Shri Rajendra Agrawal
3. Shri Raj Babbar
4. Shri Nikhil Kumar Choudhary
5. Shri Khagen Das
6. Shri A. Ganeshamurthi
7. Shri Rajen Gohain
8. Smt. Darshana Jardosh
9. Shri Baidya Nath Prasad Mahato
10. Shri Sadashivrao D. Mandlik
11. Dr. (Prof.) Thokchom Meinya
12. Shri Tapas Paul
13. Dr. (Prof.) Prasanna Kumar Patasani
14. Shri Abdul Rahman
15. Shri Radhe Mohan Singh (Ghazipur)
16. Smt. Seema Upadhyay
17. **Vacant**
18. **Vacant**
19. **Vacant**
20. **Vacant**
21. **Vacant**

**Rajya Sabha**

22. Shri Joy Abraham
23. Shri Mohammed Adeeb
24. Shri Javed Akhtar
25. Shri Salim Ansari
26. Shri B.K. Hariprasad
27. Shri Basawaraj Patil
28. Dr. Kanwar Deep Singh
29. Shri Sachin Ramesh Tendulkar
30. Dr. C.P. Thakur
31. **Vacant**

**Secretariat**

| | | | |
|---|---|---|---|
| 1. | Shri Brahm Dutt | - | Joint Secretary |
| 2. | Shri N. C. Gupta | - | Director |
| 3. | Dr. Sagarika Dash | - | Deputy Secretary |
| 4. | Smt. Rinky Singh | - | Executive Assistant |

## INTRODUCTION

I, the Chairman, Standing Committee on Information Technology (2013-14), having been authorized by the Committee to present the Report on their behalf present the Fifty-second Report on the subject 'Cyber Crime, Cyber Security and Right to Privacy'.

2. The Committee took briefing and evidence of the representatives of the Department of Electronics and Information Technology (Ministry of Communications and Information Technology) on 9th July, 2013 and 23rd August, 2013 respectively. The Committee wish to express their thanks to the representatives of the Department for appearing before the Committee for evidence and furnishing the information desired by the Committee in connection with the issues relating to the subject.

3. The Report was considered and adopted by the Committee at their sitting held on 10th February, 2014.

4. The Committee also place on record their appreciation for the valuable assistance rendered to them by the officials of Lok Sabha Secretariat attached to the Committee.

5. For facility of reference and convenience, the observations/recommendations of the Committee have been printed in bold letters in Part-II of the Report.

**RAO INDERJIT SINGH**
**Chairman,**
**Standing Committee on**
**Information Technology**

**New Delhi**
**10 February, 2014**
**21 Magha, 1935 (Saka)**

# REPORT

## PART – I
## NARRATION ANALYSIS

## CHAPTER-I
## INTRODUCTORY

### I. Overview

The emergence of the Internet in the late 1980s led to the evolution of cyberspace as a fifth domain of human activity and in last two decades, Internet has grown exponentially worldwide. India too has witnessed significant rise in cyber space activities and usage of internet so much so that it has not only become one of the major IT destinations in the world but has also become the third largest number of Internet users after USA and China. Such phenomenal growth in access to information and connectivity has on the one hand empowered individuals and on the other posed new challenges to Governments and administrators of cyberspace.

1.2 Cyber space has unique characteristics *viz*. anonymity and difficulty of attribution, coupled with enormous potential for damage and mischief. This characteristics not only adds to the vulnerabilities but also makes cyber security a major concern across the globe since it is being exploited by criminals and terrorists alike to carry out identity theft and financial fraud, conduct espionage, disrupt critical infrastructures, facilitate terrorist activities, steal corporate information and plant malicious software (malware) and Trojans. The emergence of cloud and mobile technology has further complicated the cyber threat landscape. Moreover, with the advent of sophisticated and malicious cyber tools physical damage on critical infrastructure and systems are inflicted and systematically information from targeted systems are stolen. All this makes cyber security an issue of critical importance with profound implications for our economic development and national security. Given the growing threats to cyber assets and all pervasive inter-connected information systems, countries around the world are engaged in actions for ensuring security of their cyber space.

1.3 Cyber security, a complex issue, cuts across domains and national boundaries and makes it difficult to attribute the origin of cyber-attacks. It, therefore, calls for a strategic and holistic approach requiring multi-dimensional and multi-layered initiatives and responses.

## II. Nature of Cyber Space

1.4 The Cyber Space comprises of computer systems, computer networks and Internet. The latter includes Local Area Networks and Wide Area Networks. The Internet is a network of networks spread across the globe. Commercially, these computer systems are called servers, desktops, laptops, Personal Digital Assistants (PDAs), mobile computing platforms etc.

1.5 Unlike physical space, cyber space is anonymous and borderless. Once anybody is on Internet he can access any system on Internet spread across the globe from anywhere. The cyber space offers virtual environment where anyone can hide his identity on the network and creates a pseudo name or can acquire some other identity. The security of the computer infrastructure is of greater importance under these conditions.

## III. Cyber Space usage: World and Indian scenario

1.6 The Department of Electronics and Information Technology informed that the Internet is a powerful force for good. Within 20 years it has expanded from almost nothing to a key component of critical national infrastructure and a driver of innovation and economic growth. It facilitates the spread of information, news and culture. It underpins communications and social networks across the world. A return to a world without the Internet is now hardly conceivable. A list of top 20 countries with highest number of internet users is given at Annexure I. Interestingly, India is at 3rd position with an estimated 100 million internet users as on June, 2011.

1.7 The Committee were informed that India is among the top five countries in Web Hosting. The rankings in web hosting during the years 2011 and 2012 is as under:-

| Country | 2011 Ranking | 2011 Percentage | 2012 Ranking | 2012 Percentage |
|---|---|---|---|---|
| United States | 1 | 47 | 1 | 44 |
| Greater China | 2 | 7 | 2 | 9 |
| South Korea | 3 | 7 | 4 | 8.5 |
| United Kingdom | 4 | 5 | 5 | 7 |
| Canada | 5 | 5 | 6 | 5 |
| India | 14 | 0.82 | 12 | 1.5 |

1.8 A comparative usage of cyber space worldwide and in India during the years 2005 and 2012 is as under:-

| **Cyber Space Usage** | **World wide** | | **India** | |
|---|---|---|---|---|
| | **2005** | **2012** | **2005** | **2012** |
| **Total number of websites** | 7.5 million | 698 million (registered)<br>209 million(active) | 1.7 Lakhs | 14 million<br>1.7 million '.in'(registered)<br>1 million '.in' (active) |
| **Number of Internet users** | 720 million | 2.41 billion | 21 million | 150 million |
| **Number of email accounts** | 315 million | 3.146 billion | 11 million | 180 million |

## IV. Risks in Cyber Space

1.9 As per the Background Note furnished by the Department, the risks in cyber space are manifold. They threaten personal data security-that is to say, they may undermine the individual's ability to control the information that they have entered into or stored on connective devices such as PCs, mobile telephones, or databases operated by commercial organizations, Government agencies and others. Victims typically suffer financial loss through fraud, though in cases of identity theft they may also suffer loss of reputation, or, in extreme cases, may be accused of crimes they did not commit. Online risks may also impact upon personal safety – it means that they may lead to direct physical or psychological harm to the individual. One recent high-profile threat is the one posed to children by predatory pedophiles, which conceal their true identity whilst using the Internet to "groom" potential victims. Probably far more common is the online bullying of children by their peers, while even adults who injudiciously disclose personal information online have found that their personal physical safety has been compromised and abused. As of now, it can be said that the benefits, costs and dangers of the Internet, are poorly understood and appreciated by the general public. The current assumption that it is end users' responsibility for security bears little relation either to the capabilities of many individuals or to the changing nature of the technology and the risk. The key contributors to online risks for an individual can be summarized as follows:

- Lack of knowledge
- Carelessness
- Unintentional exposure of or by others
- Flaws in technology – for instance, in the services offered online
- Criminal acts.

## V. Cyber security scenario in India

1.10 In keeping with the general trend of growth of information technology worldwide, in India too there has been tremendous growth in use of information technology in all walks of life. The internet user base has increased to 100 million and total broadband subscriber base has increased to 12.69 million. The target for broadband connections by 2014 is 22 million. Today, India has 134 major ISPs, 10 million registered domain names (1 million '.in' domains) and over 260 data centers all over the country.

1.11 Significant increase in cyber space activities and access to internet use in the country has resulted in increased opportunities for technology related crime. Coupled with this, lack of user end discipline inadequate protection of computer systems and the possibility of anonymous use of ICT – allowing users to impersonate and cover their tracks of crime, has emboldened more number of users experimenting with ICT abuse for criminal activities. This aspect, in particular, has a significant impact in blunting the deterrence effect created by legal framework in the form of Information Technology Act 2000 and other well-intended actions of enhancing cyber security in the country. As a result, today Indian cyber threat landscape, like other parts of the world, has seen a significant increase in spam & phishing activities, virus and worm infections, spread of bot infected systems. The rate of computer infections and spam & phishing activities in the country keep fluctuating, making India figure among the active sources, as is generally seen in developed economies with high rate of IT usage.

## VI. Types of Cyber crime/attack - methodology and impact

1.12 Most of the Internet frauds reported in the country are relating to phishing, usage of stolen Credit Cards / Debit Cards, unauthorized fraudulent Real Time Gross Settlement (RTGS) transactions, fictitious offers of funds transfer, remittance towards participation in lottery, money circulation schemes and other fictitious offers of cheap funds etc.

1.13 When the Committee desired to know the mode of occurrence and prevention of various types of cyber-crimes existing/emerging around the world and in our country, the Department, in their written reply, furnished the following information:-

| Sl. | Type of | Definition | Mechanism in | How it can be prevented/tackled |
|---|---|---|---|---|

| No | cyber Crime | | which it is carried out | Legal Measures as per Sections Relevant in IT Act, 2000 and Amendments | Technical and other Measures |
|---|---|---|---|---|---|
| 1 | Cyber Stalking | Stealthily following a person, tracking his internet chats. | By using electronic communication, such as e-mail instant messaging (IM), messages posted to a Web site or a discussion group. | 43, 66 (Compensation and punishment of three years with fine) | Not disclosing personal information on Internet, chat, IM and interacting over electronic media with known people only. Taking up the matter with concerned Service Providers in stopping cyber stalking activities. |
| 2 | Intellectual Property Crime | Source Code Tampering etc. | Accessing source code or such type of material and stealing or manipulating the code etc. | 43, 65, 66 (Compensation and punishment of three years with fine) | Strong authentication and technical measures for prevention of data leakage |
| 3 | Salami Attack (Theft of data or manipulating banking account) | Deducting small amounts from an account without coming in to notice, to make big amount | By means of unauthorized access to source code of software application and databases | 43, 66 (Compensation and punishment of three years) | Strong authentication measures for accessing the data and securing the IT infrastructure involved |
| 4 | E-Mail Bombing | Flooding an E-mail box with innumerable number of E-mails, to disable to notice important message at times. | Bulk email generation to target specific email account by using automated tools | 43, 66 (Compensation and punishment of three years) | Implementing anti-spam filters |
| 5 | Phishing | Bank Financial Frauds in Electronic Banking | Using social engineering techniques to commit identity theft | 43, 66, 66C (Compensation and punishment of three years with fine) | Immediate take-down of phishing websites.<br>Strong authentication mechanisms for financial and electronic banking. User awareness on phishing attacks<br>Keeping the computer systems secure being used for transacting with the financial |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | institutions and banks. |
| 6 | Personal Data Theft | Stealing personal data | Compromising online personal data, email accounts and computer systems | 43, 43A, 72A (Compensation and punishment of three years with fine) | Safeguarding the online data and personal computer systems |
| 7 | Identity Theft | Stealing Cyberspace identity information of individual | Hacking the personal identity information or employing phishing techniques | 43 (Compensation and punishment of three years with fine) | Safeguarding of personal identity information, securing the personal computer systems, awareness on preventing identity theft and adopting safe internet practices |
| 8 | Spoofing | Stealing Credentials using, friendly and familiar GUI's | Using tools and other manipulative techniques | 43, 66 (Compensation and punishment of three years with fine) | Safeguarding the credentials and implementing anti-spoofing measures |
| 9 | Data Theft | Stealing Data | Hacking of computer systems and using malicious methods | Provisions under 43, 43A, 65,66 and 72 (Compensation and punishment of three years with fine) | Securing the computer systems, implementing data leak prevention measures and creating user awareness |
| 10 | Worms Trojan Horses, Virus etc. | Different Hacking mechanisms | Different methods to install and propagate malicious code | 43, 66 (Compensation and punishment of three years with fine) | Securing computer systems, installing anti-malware systems and creating user awareness. |
| 11 | Sabotage of Computer | Taking control of computer with the help of malware. | Compromising the computer systems | 43, 66 (Compensation and punishment of three years with fine) | Securing computer systems and deploying anti-malware solution |
| 12 | DOS, DDOS Demat of Service | Flooding a computer with Denial of Service Attacks, DDOS is Distributed DOS attack | Generating flood traffic from thousands and millions of compromised computers using automated tools and techniques | 43, 66, 66F (Compensation (up to life imprisonment under 66F) | Implementing DOS, DDOS prevention systems |

| | | | | | |
|---|---|---|---|---|---|
| 13 | Web Defacing | Web Pages Defacing | Compromising the websites and adding or manipulating the web pages with some messages | 43, 66 (Compensation and punishment of three years with fine) | Securing the websites and the IT infrastructure used for hosting and maintaining the websites |
| 14 | Spam and spoofing | Unsolicited E-mails | Sending unsolicited emails through manual and automated techniques | 43, 66A, 66D (Compensation and punishment of three years with fine) | Deploying the anti-spam and anti-spoofing solution at email gateways |
| 15 | Publishing or transmitting obscene material | Publishing Obscene in Electronic Form | Publishing or transmitting the obscene content over electronic media like websites, social networking sites etc. | 67 (Punishment of three years with fine) | Taking down of obscene materials over electronic media |
| 16 | Pornography | Publishing or transmitting material containing sexually explicit act | Publishing pornographic material over electronic media like websites, social networking sites etc. | 67A (Punishment of five years with fine) | Taking down of pornographic material publishing websites/ web-pages, online media etc. |
| 17 | Child Pornography | Publishing Obscene in Electronic Form involving children | Publishing pornographic material involving children over electronic media like websites, etc. | 67B | Taking down of pornographic material publishing websites/ web-pages, online media etc. |
| 18 | Video Voyeurism and violation of privacy | Transmitting Private/ Personal Video's on internet and mobiles | Transmitting Private/Personal Video's on internet and mobiles | 66E (Punishment of three years with fine) | Taking down of such content as available over internet and transmitted through mobiles. |
| 19 | Offensive messages | Communication of offensive messages through computer/ phone | Sending or publishing the offensive messages over electronic media like email, websites and social media | 66A (Punishment of three years with fine) | Taking down of offensive messages from electronic media and creating user awareness on safe internet practices |
| 20 | Hacking of Protected Systems | Protection of Information Infrastructure | Hacking the computer systems by using various methods | 70 (Punishment of ten years with fine) | Securing the computer systems and related infrastructure, creating user awareness and training of system administrators |

## CHAPTER-II

## GROWING INCIDENTS OF CYBER CRIME AND FINANCIAL LOSS

1.14 Of late Indian cyber space has witnessed significant rise in cyber-attacks/fraud, massive probing and targeted attacks on IT assets are being witnessed. The Indian cyberspace is also being used to host Command and Control Servers in the data centres. Attempts have been noticed to attack telecom infrastructure particularly, the routers and DNS. There have been cyber attacks on the Government, public sector and private sector IT infrastructures like website defacements, intrusions, network probing, and targeted attacks to steal some information, identity theft (phishing) and disruption of services. About 300 end user systems on an average are reported to be compromised on a daily basis. More than 100,000 viruses/worms variants are reported to be propagated on the net on a daily basis, of which 10,000 are new and unique. The malicious codes are easily available on the net and their cost varies from a few dollars to a few thousand dollars depending upon the purpose and sophistication. The infrastructure hosting, collecting and propagating malicious activities are offered on lease / rent basis.

1.15 As per the information provided by the Department for the last five years the number of reported incidents of website compromise has grown 5.5 times and India is today among the first five countries with respect to spam mail. Based on the incidents reported to CERT-In in the past five years (2007-12) the phishing incidents have increased from 392 to 887 and in the year 2013 (till February), a total of 110 Phishing Incidents have been observed.

1.16 The Department has furnished the following data on the total number of websites defaced/hacked during the last five years:-

| **Numbers of Indian and world-wide websites defaced / hacked** | | **2008** | **2009** | **2010** | **2011** | **2012** | **2013 (upto February)** |
|---|---|---|---|---|---|---|---|
| **World wide** | **Websites defaced/hacked** | 517459 | 544409 | 1419202 | 1612728 | 1274162 | Data not yet available |
| | **Government/ Strategic Organisations' websites defaced/hacked** | 9606 | 11929 | 16875 | Data not available | Data not yet available | Data not yet available |
| **India** | **Websites defaced/hacked** | 6310 | 12161 | 20701 | 21699 | 27605 | 3911* |
| | **Government websites defaced/hacked** | 90 | 201 | 303 | 308 | 371 | 40* |

** Upto June 2013 the no. of total Websites defaced/hacked was 12693, of which Government websites are 78 and other 12615*

1.17 Number of Central and State Government websites registered with 'gov.in' domain is 8200 and number of Government websites hosted by NIC is 7137. Details of domain wise break-up of Indian websites defaced/hacked in the last five years as per information furnished by Department are as under:-

| | **2008** | **2009** | **2010** | **2011** | **2012** | **2013** |
|---|---|---|---|---|---|---|
| **.in** | 4387 | 8979 | 15823 | 13924 | 15524 | 2667 |
| **.gov.in and nic.in** | 90 | 201 | 303 | 308 | 371 | 40 |
| **.com** | 1416 | 2446 | 3854 | 6335 | 10320 | 1055 |
| **.org** | 235 | 238 | 447 | 663 | 754 | 84 |
| **.net** | 142 | 166 | 221 | 311 | 436 | 46 |
| **others** | 40 | 131 | 53 | 158 | 200 | 19 |
| Total | **6310** | **12161** | **20701** | **21699** | **27605** | **3911** |

1.18 The number of cyber threat incidences in the country, from the year 2004 upto September, 2013 as per CERT-In was as under:-

| **Activities** | **2004** | **2005** | **2006** | **2007** | **2008** | **2009** | **2010** | **2011** | **2012** | **2013 (Sep)** |
|---|---|---|---|---|---|---|---|---|---|---|
| **E-mail messages received** | 625 | 1822 | 1948 | 3283 | 4073 | 8050 | 13825 | 22754 | 44520 | 27909 |
| **Incidents handled** | 23 | 254 | 552 | 1237 | 2565 | 8266 | 10315 | 13301 | 22060 | 42434 |
| **Security Alerts/ Incident Notes** | 20 | 30 | 48 | 44 | 49 | 29 | 43 | 48 | 10 | 11 |
| **Advisories** | 23 | 25 | 50 | 66 | 76 | 61 | 73 | 81 | 56 | 72 |
| **Vulnerability Notes** | 74 | 120 | 138 | 163 | 197 | 157 | 275 | 188 | 122 | 178 |
| **Security Guidelines** | 4 | 2 | 1 | 1 | 1 | | 1 | 4 | - | - |
| **White Papers/Case Studies** | 3 | 6 | 2 | 2 | 3 | 1 | 1 | 3 | - | - |
| **Trainings** | 7 | 6 | 7 | 6 | 18 | 19 | 26 | 26 | 26 | 17 |
| **Indian Website Defacement tracked** | 1529 | 4705 | 5211 | 5863 | 5475 | 6023 | 14348 | 17306 | 23014 | 19886 |
| **Open** | 236 | 1156 | 1837 | 1805 | 2332 | 2583 | 2492 | 3294 | 2759 | 1587 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Proxy Servers tracked Bot Infected systems tracked** | - | - | - | 25915 | 146891 | 2159804 | 6893814 | 6277936 | 6494717 | 5917695 |
| **Security Drills** | - | - | 1 | 2 | 2 | 3 | 4 | 4 | 6 | 1 |
| **Security Audits** | - | - | - | - | - | 13 | 15 | 19 | 6 | 16 |

1.19 On the increasing threat in cyber space and the Government's action plan to tackle the issue, the Secretary, Department of Electronics and Information Technology (DeitY), during the course of evidence submitted as under:

> "Now, as you have rightly said, the nature and size of the threat in the cyber space is increasing in India, especially with 150 million plus Internet users and a large e-governance sector which is providing a large number of Government to citizen and Government to business services. In addition, 11 critical sectors, which predominantly use Information Technology as part of their operations, whether it is power, atomic energy, space, aviation, transportation etc., have also become more important to protect the information and assets in these areas. In the Documentation Survey, we have identified and submitted to you 20 different categories of threats looming around us and against which we have to protect the whole cyber space. Again, as you have rightly pointed out, a number of reported crimes and the number of reported incidents are on the increase year to year. This shows that we need to put in a more concerted effort at this point of time. That has led the Government to come out with an overall framework for the National Cyber Security and also a specific policy. While the framework is cross-cutting in nature, it applies across several major Ministries and sector. So, that is being looked after by the National Security Council Secretariat (NSCS) whereas the Cyber Security Policy is the responsibility of the Department of Information Technology. That is how it has been worked out and the policy has again identified certain priority areas because not everything can be done overnight. So, certain priority areas have been identified."

1.20 In the context of increasing incidents of cyber crime, the Committee desired to know about the anticipated quantum loss of money and time if the country is subjected to a cyber attack to which, the representative of the Department submitted during evidence as under:

> "Our nuclear establishments are well protected. Atomic Energy Commission and others have taken adequate steps. But in many other areas, the solace is that our systems are not on the Internet. Even the atomic energy we have air gap between the system, internal infrastructure and elsewhere. But at the same time, we have proposed the 24X7 National Critical Information Infrastructure Protection Centre.

We are trying to implement best practices so that if any attacks happen as we go on, we are able to face it. Particularly the power sector, fortunately their systems are not internally (within the country) connected; now with modernisation and modern technology, systems are being built up but there are issues. We may not face such kind of attacks because of the less integration."

1.21 In this regard, the Secretary of the Department added as under:

"In security equipment, even though it is not connected to Internet, there are other possibilities like it may have some hidden malware, embedded software because several things we are importing. It may not be connected to Internet but on a triggered date, as happened in Stuxnet, etc. Also, it kicks off certain activities and sends messages out. One of the priority items is to beef up our own security testing infrastructure. We have one in Kolkata. We need to expand several fold – both for us and telecom."

1.22 The Department has submitted that as per the data maintained by National Crime Records Bureau (NCRB) on cyber-crime, a total of 420, 966, 1791 and 2876 Cyber Crime cases were registered under Information Technology Act during 2009, 2010, 2011 and 2012 respectively, thereby showing an increasing trend. A total of 276, 356, 422 and 601 cases were registered under Cyber-Crime related sections of Indian Penal Court (IPC) during 2009, 2010, 2011 and 2012 respectively. In addition, number of Cyber Crime cases registered by Central Bureau of Investigation (CBI) during the years 2010, 2011 and 2012 under provisions of Information Technology Act 2000 and other Acts were 10, 12 and 11 respectively. Further, with regard to the data pertaining to the privacy related cases and persons arrested as per NCRB during the years 2010, 2011 and 2012 are as follows:-

| **Sl. No** | **Crime Head** | **Cases Registered** | **Persons Arrested** | **Cases Registered** | **Persons Arrested** | **Cases Registered** | **Persons Arrested** |
|---|---|---|---|---|---|---|---|
| | | **2010** | | **2011** | | **2012** | |
| **1** | **Breach of confidentiality / privacy (Section 72(A))** | 15 | 27 | 26 | 27 | 46 | 22 |

1.23 When the Committee desired to know the quantum of financial loss to the country due to cyber-attack/fraud in last five years, the Department, in their written reply, stated that according to Reserve Bank of India (RBI), the number of fraud cases as reported by Banks on account of ATM Debit Cards / Credit Cards / Internet have decreased from 15018 (in 2010) to 8322 (in 2012). However, the amount involved had increased from Rs. 40.48 crore in the year 2010 to Rs. 52.66 crore in the year 2012. Central Bureau of Investigation (CBI) has also registered cases pertaining to financial

frauds under the provisions of Information Technology Act 2000 along with other Acts which are as follows:-

| Year | No. of Cases | Amount Involved in crore (Rs. in Crore) |
|---|---|---|
| **2010** | 6 | 6.42 |
| **2011** | 10 | 12.43 |
| **2012** | 8 | 28.79 |

1.24 On the issue of maintenance of data of cyber fraud the Department, in their written reply stated that National Crime Records Bureau (NCRB) under Ministry of Home Affairs (MHA) is maintaining data on cyber frauds. Accordingly, MHA has been requested to advise NCRB to maintain data with regard to disposal status of registered cyber-crime cases. The mechanism for recording data with regard to Internet financial frauds, along with quantum of loss, is being maintained by Reserve Bank of India and Central Bureau of Investigation (CBI). DeitY regularly interacts with Banks, RBI and CBI regarding cyber fraud incident related actions such as prevention, investigation support, technical advisories, promotion of best practices and compliance. As a result, RBI has advised banks and financial institutions to follow the advisories of CERT-In and notify the incidents to CERT-In as and when they occur.

## CHAPTER-III

## CHALLENGES/ CONSTRAINTS

1.25 The cyber threat landscape is dynamic and evolving with innovative technologies, techniques and actors and offenders are well versed with technology and they are exploiting the lack of situational awareness of defenders. Cyber threats like espionage and Denial of Service (DoS) attacks to offensive actions by adversarial State and Non-State actors. Several countries are developing sophisticated malicious codes as lethal cyber weapons. Large scale mapping of SCADA (Supervisory Control and Data Acquisition) devices using specialized tools, pose major challenge for any country.

1.26 DeitY, in their background note, has outlined the following as the main issues and challenges observed in the cyber space:-

- Expanding role and implementation of Information Technology across all sectors in the country
- Growth in volume and complexity of Information Technology ecosystem in the country
- Growth in volume of transactions and sensitive data exchange
- Rapidly changing security and threat landscape
- Paradigm shift in attack vectors and nature of their launch
- Difficulty in tracing origin of attack
- Need for reducing cyber security risk exposure of IT infrastructure and ecosystem in the country
- Responsibility to ensure that proper processes, technology, governance structure and compliance to laws and regulatory requirements are followed in a borderless environment
- Defending borderless environment poses challenges which are dynamic in nature.

1.27 During the course of evidence, the Department in their power point presentation, highlighted some more challenges, which are as under:-

**Cyber Crime, Espionage, Cyber Sabotage / Subversion, Cyber Terrorism**

| Technical | Individual and Business |
|---|---|
| • Malware (including virus, trojan, keyloggers, etc.)<br>• Unprotected Wireless Network<br>• Untrusted / rogue devices and media<br>• Product (hardware and software) backdoors | • Identity Theft (including phishing, Duplicate and unauthorized Digital Certificates, etc.)<br>• Insecure IT Applications (including Denial of Service, Defacement, Backdoors, etc.)<br>• Operational vulnerable systems (including Bot command and controls, Rootkits, etc.)<br>• Social Engineering |

| National | Societal |
|---|---|
| • Backbone Denial of Service / DDoS | • Hactivism |
| • Advanced Persistent Threats | • Culture Jamming |
| • Steganography | • Electronic civil disobedience |
| • Critical Infrastructure sabotage | |

1.28 The Department also informed DDoS attacks, Anonymous attacks – groups sponsored by Nations and terrorist groups, Traffic highjacking, Espionage, Social Networking sites for electronic civil disobedience, etc. as some of the major cross border challenges in cyber security scenario.

## I. Lack of adequate human resource to tackle the challenge (Auditors, Experts, Skill development in IT)

1.29 The Department has informed that all critical sector organizations under central Government Ministries/Departments are mandated to implement information security best practices as per ISO 27001. So far, 546 organizations in the country have obtained ISO 27001 certification. Organisations in the other sectors are also taking steps to implement these best practices.

1.30 During the examination of Demands for Grants (2011-12) and (2012-13), the Department had repetitively submitted that there is shortfall of cyber auditors/experts/IT skill in the country and therefore, their HRD activities are targeted to ensure availability of trained human resources for the manufacturing and service sectors of electronics and IT industry. Such initiatives include identifying gaps emerging from the formal sector and planning programmes in non-formal and formal sectors and action for meeting these gaps.

1.31 In this context, the Committee desired to know the details of the existing manpower in the country so as to mitigate challenges of cyber threat. To this, the Department, in their written reply submitted as under:

> "The efforts of the Department by way of implementing a national Information Security Education and Awareness Project (ISEA) has resulted in development of cyber security related man power as well as master trainers in the country. So far around 42,000 students have been trained/undergoing training in various long-term/ short-term courses at various levels….xxxxxx.."

1.32 In response to a query on the challenges in cyber security, the Department, in their written reply stated that shortage of manpower is one of the major constraints in all the organisations involved in securing Indian cyber space. Critical shortage of cyber security professionals need to be tackled in mission mode with innovative recruitment and placement procedures along with specialized training of existing manpower.

1.33 When the Committee desired to know whether there was any plan to increase the number of cyber security experts in the Indian Government organisations, the Department, in their written reply stated as under:-

> "In order to increase the number of cyber security experts in Indian Government organizations, extensive training programmes have been conducted as part of the Information Security, Education and Awareness Programme (ISEA) of the Department..xxxxxx.. In addition, the National Security Council Secretariat is already engaged with the task of determining the extent of augmentation in the number of Cyber Security experts in the Govt. Organizations."

1.34 During the evidence on the subject, the Secretary, DeitY added as under:-

> "...xxxxx.. For everything, we need skilled manpower because the country is large and our problems are different and complex. So, a continuous programme of capacity building and training is going on. So far 42,000 students of engineering and computer sciences have been taken through a special course, short-term and medium-term course as they are doing their B. Tec., M. Tec. or Ph.D, this course was also done side-by-side by them in a programme called IESA. In the current year also we are continuing that programme and we want to enhance that because the ultimate requirement of manpower is reported to be about 5 lakh in this country. About 42,000 have been trained and along with the existing people we are somewhere in the region 65,000 but a long way to go to five lakhs...xxxxxxx.."

1.35 Asked as to what is the number of auditors empanelled by CERT-in in the country, the Department, in their written reply, submitted as under:-

> "There are 44 empanelled auditors by CERT-In for purpose of carrying out cyber security audit related activities.
>
> National Informatics Centre (NIC) has the process of engaging CERT-In empanelled auditors to carry out auditing of Government web sites. These audits are conducted prior to hosting of a Government website on NIC infrastructure. Subsequently audits are also conducted on periodic basis especially following major changes/ upgradation in ICT infrastructure."

1.36 Elaborating it further, the Director-General, CERT-In, stated during evidence:-

> "The process is always open and more auditors can get themselves empanelled. We follow a very stringent process in appointing the auditors. We first give them a CD of vulnerabilities. They detect the vulnerabilities. They report to us. If they are able to report 90 per cent vulnerabilities or the problems in a software, then we ask them to go for an on line test. They have to pass the on line test with 95 per cent detection. Only when they give 95 per cent, then we empanel them. So we follow a very stringent process. Thereafter, we go for the verification, the credentials of the manpower who do the auditing. It goes to the Ministry of Home Affairs and the proper process of verification and identification is gone through. The entire process takes six months to empanel auditors and the process is on. The auditors are again asked to go for the test after a year there. We cannot take the approach that once you empanel them you can forget about it. Every year they have to pass the test. That is why at one point of time we had 87 auditors and we brought the list down to 42 because they have to pass this stringent test. This process is on, as I mentioned."

## II. Infrastructure and Research and Development to secure Cyber Space

### (i) Research and Development

1.37 Research and Development (R&D) initiative is essential for development/enhancement of skills and expertise in areas of cyber security by facilitating basic research, technology demonstration and proof-of-concept and R&D test bed projects. Research and Development is carried out by the Department in areas of cyber security including (a) Cryptography and cryptanalysis, (b) Network & System Security, (c) Monitoring and Forensics and (d) Vulnerability Remediation and Assurance through sponsored projects at recognized R&D organisations and academic institutions.

1.38 The Department of Electronics and Information Technology (DeitY) has informed that it has set up a Sub-Group on Cyber Security for Twelfth Five Year Plan on Information Technology Sector, consisting of various experts/ representatives from academic and R&D Organisations, Industry and user agencies, which has deliberated on various issues related to Cyber Security R&D and has identified key priorities for R&D which *inter-alia* include to carry out innovative R&D with focus on basic research, technology development and demonstration, setting up test-beds, transition, diffusion and commercialization leading to widespread deployment in the field to enhance security of cyber space in the country.

1.39 The details of funds allocated for R&D under Cyber Security Programme for last 5 years and the expenditure incurred, as provided by the Department, are as under:-

Rs. in crores

| Sl.No. | Year | Funds allocated | Expenditure |
|---|---|---|---|
| 1. | 2009-10 | 15.0 | 15.0 |
| 2. | 2010-11 | 22.5 | 21.2 |
| 3. | 2011-12 | 25.0 | 25.0 |
| 4. | 2012-13 | 25.00 | 14.01 # |
| 5. | 2013-14 | 26.97 | 15.73 (upto 20.1.2014) @ |

**#** The funds flow to the projects has taken time due to procedural compliance for settling of pending UCs of other programmes and hence funds could not be utilized fully.

**@** The budget has been cut down by Rs. 10 crore (approx)

1.40 On being asked whether R&D in Cyber Security is sufficient to meet the upcoming challenges in Cyber Space, the Department in a post evidence reply stated as under:-

> "……..x..x..x…. the actions (taken by the Department) have significantly contributed to the creation of a platform that is capable of supporting and sustaining the efforts to securing the cyber space. However, due to the dynamic nature of cyber threat scenario, these actions need to be continued, refined and strengthened from time to time.
> …..x..x..x..Present funding provided to R&D in the area of Cyber Security does not allow undertaking projects for development of strategic technologies."

1.41 Asked as to whether there is any proposal for improving the R&D scenario in Cyber Security in India, the Department in their post evidence reply further stated that the Government has published the 'National Cyber Security Policy' on 2nd July 2013, to address the cyber security challenges with an integrated vision and a set of sustained and coordinated strategies for implementation. Further, Cyber Security R&D is one of the key components of the National Cyber Security Policy with an objective 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. According to the Department the Cyber Security R&D objective of the National Cyber Security Policy is sought to be supported by the following strategic actions:

a. To undertake Research and Development Programs for addressing all aspects of development aimed at short term, medium term and long term goals. The Research and 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.

b. To encourage research and development to produce cost-effective, tailor-made indigenous security solutions meeting a wider range of cyber security challenges and target for export markets.

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

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

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

f. Large funds need to be allocated to undertake development of key technologies.

DeitY has constituted a Working Group with experts from Academic/ R&D organisations, Govt and user organisations to provide advisory support for implementation of Cyber Security R&D programme.

### (ii) Cyber Crime Cells and Cyber Crime Labs

1.42 On being enquired about the cyber crime cells and labs in the country, the Department in their written submission stated as under:-

> "Ministry of Home Affairs under the Cyber Crime Investigation programme, is supporting the establishment of Cyber Crime Police Station (CCPS) and Cyber Crime Investigations and Forensic Training Facilities (CCIFTF) in each State / Union Territory of India under Police Modernization Scheme.
>
> Cyber forensics training lab has been set up at Training Academy of Central Bureau of Investigation (CBI) to impart basic and advanced training in Cyber Forensics and Investigation of Cyber Crimes to Police Officers associated with CBI. In addition, Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States. In collaboration with Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs have been set up at Mumbai, Bengaluru, Pune and Kolkata for awareness creation and training programmes on Cyber Crime investigation."

1.43 To a related query on the functions of the lab, the Department informed that cyber Forensics Laboratory is designed to execute a number of forensic activities. These activities can be broadly categorised in (1) Computer Forensics, (2) Network Forensics and (3) Mobile Forensics. Its main functions are training on cyber crime and cyber forensic evidence.

1.44 On the issue of cyber crime cells in States, the representative of the Department during the evidence stated as under:

"Every State has opened the cyber crime cell. Some States have one cyber cell and considering the size of the State, some have more than one, to address such crimes. All these cells follow the same Cr.P.C. There is no separate Cr.P.C. for cyber crimes. They follow the same Cr.P.C. which is followed for the conventional crimes. We have prepared manuals on how to analyse the cyber crimes and how to put up the cases to courts. These manuals have been given to all the Police Departments…xxx…….xxx…..xxx… Manuals have been given so that they follow the uniformity of the process. The issue comes up because the Cr.P.C. is followed uniformly and the police authorities are well conversed with the Cr.P.C. But the issue areas in investigation oc cyber crimes, where much more training needs to be given to the police officials to handle such cases – first of all, how to collect the evidence. Though we have given the manuals, how to analyze the evidence and how to relate those evidence with other evidences, and to put up to the courts. These are the three issues which need to be seen. We have given the manuals; we are working with the Bureau of Police Research and Development to give more training. Not only this, in almost ten States, we have given funds and opened cyber labs so that the police officials can be trained. In all the north eastern States where the cases are coming up, we have opened lab in every State, depending upon the size of the State, sufficient police officials have been getting training; not only we have taken a project, with the help of the judiciary, we are trying to train the judges also, how to read those evidences; the training for them is currently in process. The intention is to have a uniform process because any cyber crime may or may not be linked to only one State; it may have a link to a number of States and maybe, outside the country also. So, the purpose is to have a uniform process, but we need to go far ahead in terms of training the police officials."

## III. Budgetary allocations to tackle the Cyber threats

1.45 The Department has furnished the following data on the budget allocated and utilized in Research and Development (R&D) for cyber security for the last six years (2007-08 to 2013-14):-

(Rs. in crore)

| Year | Budget allocated | Utilised |
|---|---|---|
| 2007-08 | 33 | 22.74 |
| 2008-09 | 33 | 31.07 |
| 2009-10 | 33 | 29.64 |
| 2010-11 | 40 | 35.45 |
| 2011-12 | 45.2 | 39.95 |
| 2012-13 | 45.2 | 30.87 |
| 2013-14 | 54.37 | 6.24 (upto June 2013) |

1.46 When asked as to whether the allocations made for cyber security programme were adequate, the Department, in their written reply, stated as under:-

"The allocations for Cyber Security Programme are in line with the Department's total allocation. The key objectives envisaged by the Department are part of the report of the Sub-Committee on cyber security for the 12th Five-Year Plan, which has been accepted by the Planning Commission. Considering the importance of cyber security DeitY had projected a provision of Rs. 1500 Crore for execution of the 12th Plan. However, at present an allocation of Rs. 500 Crore has been made for cyber security related activities of DietY in 12th plan. The Planning Commission has been briefed about the key initiatives of the policy and its funding requirements during Plan as well as Annual Plan discussions. More funds are required during 12th Plan period."

1.47 The Secretary, during the course of evidence, further submitted as under:-

"In the current plan (Twelfth Five Year Plan) we have earmarked Rs. 500 crore for cyber security and while that is not fully adequate to take care of all the requirements but our attempt is to get the schemes approved first, at least, to the tune of consuming this Rs. 500 crore and go to the Planning Commission with a request to allocate more funds."

## IV. Threat emerging from servers hosted outside India

1.48 The Department has stated that majority of the websites of commercial, NGOs, individuals and private organizations are hosted outside India and hosting of sites outside India is largely on account of economical and cost advantage reasons. The protection mechanism for securing websites involves significant expenditure.

1.49 When asked about the hassles being witnessed due to location of internet servers outside country, the Department, in their written reply stated that with the growing sophistication in technology, it is very difficult and challenging to positively attribute the origin of attack and to ascertain the identity of the perpetrator. Even though some of the cyber threats in the form of cyber attacks have been observed to be emanating from cyber space from across the border, conclusive attack attribution is very difficult. In view of the legal jurisdictions of different countries and entities, invariably results in legal and cooperation issues emerging out of cyber incidents/attacks/crimes, delaying the resolution and affecting the investigation process.

1.50 When enquired about the plans to address the issues arising due to location of internet, the Department, in their written reply, submitted that the action plan and strategy of the Government to deal with the issue include issuing advisory to all intermediaries including national and international service providers; maintaining regular dialogue with the intermediaries; awareness campaign on the issue; use of existing legal provisions of Information Technology Act 2000; building/updating both legal and technical safeguards to prevent the misuse of Internet. In addition,

Government has notified a 'Framework and Guidelines' for use of Social Media by its agencies. It will help the Government to interact with the common citizens and disseminate information and at the same time effectively counter the spread of hate mails and malicious information.

1.51 On the issue of hosting of servers in the country, the representative of the Department stated during evidence as under:-

> "…xx….xx….xx… our policy is to encourage the hosting of servers in India. The famous email providers like Google and yahoo, have also created services like co.in, whether it is yahoo.co.in or gmail.co.in. So, our policy is to set up facilities in India. In fact, yahoo.co.in server is located in Mumbai. Rediff has hosted server in Mumbai. Indiatimes has hosted the servers in India and they have servers outside also, they are bringing the servers to India. So, our efforts are there that the Indian data should remain in the country and the servers should be in the country, and the citizens should be able to access services in India.
>
> As far as the Government data is concerned, it is there in the NIC server which is hosted in India at Delhi and partly in other cities of the country there. As Secretary has mentioned, in regard to e-mail policy, the Foreign Missions are also being mandated that they should host a website wherever possible in India in the NIC mail servers and they should use the NIC Mail server so that they are able to prevent such cyber crimes happening against the Government."

1.52 Elaborating on the threat posed by hosting servers outside India the Secretary, during evidence, stated as under:-

> "The confidential and nationally sensitive data etc. in 99 per cent of the cases will reside and emanate from the Government organisations. So, if they choose to use servers outside the country, obviously the data will go out and reside there. ..x..x…x.. I had explained ..x..x…x.... about the intention of the Government of India to come out very shortly with a draft e-mail policy and data storage policy for the entire Government of India and the State Governments. The draft copy of the policy has been submitted to the Committee. Not only it mandates all Government employees to use the Government mail services, but it prohibits usage of private services hosted whether in India or abroad."
>
> x..x…x..x… x..x… x..x… x..x…x..x.. x..x…x..x..
>
> We are coming out with a comprehensive policy on e-mails related to information, messaging system and handling of such secret communications for entire Government. That policy is at a very advanced stage and within 8 to 10 weeks, we will be able to pass it. I would like to read out one paragraph from page 5 of that document: 'It is mandatory for the Government of India officials stationed at Embassies or working in Missions abroad/deputations to use static

IP addresses/virtual private networks/one time passwords for accessing Government of India e-mail services.' This is imperative in view of the security concerns that exist in other countries. There are many other provisions but I am pointing out only one of them. This is a comprehensive policy and we are working on it. This is called E-mail Policy of the Government of India. We will be confining it to only indigenous operations…..xxxx…..xxxxxx…….xxxxxxxx……xxxx

The second aspect is the usage of internet, especially in the Government place. When a private citizen uses internet in his or her own way we cannot say that he or she will use the internet but using the Government networks you are exposing our own system to the outside world. Therefore, necessary precaution, especially the security point of view precaution has to be taken. As a supplement to the earlier policy we have brought out this policy which is called the Acceptable Internet Usage Policy, for what purposes you can use internet and for what purposes you cannot, etc. This will bring out this policy together with e-mail and both will be processed very soon and strengthen our own defence considerably because these are the weak points for the Government. So, we are going to come out soon. My estimate would be that it should be about eight to ten week's time because inter-ministerial consideration has to be done before we issue policy because it should be applicable to all Ministries."

## V. Challenge posed by imported electronics/IT products

1.53 The Standing Committee on Information Technology in their Twenty-third Report on Demands for Grants (2011-12) and Thirty-fourth Report on Demands for Grants (2012-13) had highlighted about threat posed due to imported electronics/ IT products. When the Committee enquired about the existence of any Cell/ Organisation/ lab in India to check all imported electronics/IT/telecom products for possible security threat, the Department, in their written reply, submitted as under:-

"Under the Common Criteria Project of DIT, STQC has established the Indian Common Criteria Certification Scheme (IC3S) at STQC, New Delhi and a full-fledged laboratory at Kolkata, with a capability for testing and certification of security of IT Products as per International standard, ISO/IEC 15408, based on Common Criteria Standards up to EAL4.

The laboratory for Common Criteria evaluation is designed as per the international requirements for such facilities and meets the criteria of laboratory system as per ISO/IEC 17025 and Common Criteria standards. It has achieved international accreditation by A2LA, the accreditation agency of USA, for its evaluation practices.

Presently, evaluations are undertaken for certification of IT products like operating systems of routers, switches and firewalls; security appliances upto EAL4.

In view of the increasing penetration of ICT in the country, STQC Directorate has initiated steps to expand its facilities and enhance its capacity for testing of IT products as part of its action in 12th Plan. In addition, the sub group on testing & certification infrastructure under the Joint Working Group (JWG) for public private partnership on cyber security also envisage setting up of such testing infrastructure with active participation of private sector. In addition, Department of Telecom has also initiated steps to set up facilities for testing of Telecom products."

1.54 Highlighting further about the developments with regard to testing of electronics/telecom equipments, the Secretary, during evidence, submitted as under:-

"Another important development ...x..x..x...(with respect to) the testing of electronic equipment, telecom equipment etc. from the security perspective. ..x..x..x... we are happy to tell you that India is likely to get in another 10 days away, on 10th of September the final verdict will be released. But we are reasonably sure that we get the status of the certifying nation for electronic products in terms of security testing. So this is the CCRA, a common criteria regime that will there. Previously we were only testing as consuming nation but now we will be certifying nation. That means the certificates issued by us will be valid across the globe. So the process will end on 31st of August in a week or so from now and then on the 10th of September they are going to call us to USA. One of our representatives will go and hopefully receive the certificate which will be really a milestone in the area of security as far as their market practice is concerned for security testing."

1.55 On being enquired about the present status of India as certifying nation, the Department, in their post-evidence reply submitted as under:-

"India recognized as "Authorizing Nation" under Common Criteria Recognition Arrangement (CCRA) after the successful audit of Indian Common Criteria Certification Scheme (IC3S) being operated by STQC Directorate, Deity. India becomes the 17th nation to earn this recognition out of the total 26 member countries including USA, UK, Germany, France, Japan and South Korea etc. of CCRA as announced at International Common Criteria Conference in Orlando, USA on 10th September, 2013. Now the product tested and certified under Common Criteria Certification Scheme up to Assurance Level 4 (EAL4) are acceptable not only in India but also in other member countries of CCRA without re-testing under the mutual recognition arrangements.

STQC Directorate, established infrastructure and made operational testing and certification of security of IT products as per Common criteria standards (ISO 15408) for evaluation up to assurance level EAL4. STQC on behalf of DeitY has signed Common Criteria Recognition Arrangements (CCRA).

The present scope of Certification is limited to Network Boundary Protection Devices and General Purpose Operating Systems. It is proposed to expand the capacity and capability for testing and Certification as per Common Criteria

Standards. The area of technologies to be taken up for certification would be around the present expertise and experience of the test laboratories. The Common Criteria evaluation requires knowledge and understanding of not only about the Common Criteria standards but also the relevant technological areas. STQC does not have necessary expertise and knowledge in highly complex products, such as Radar etc. However, STQC does have the necessary knowledge in Common Criteria standards and methodology, which can be shared with other organizations.

The Common Criteria Test Laboratory at STQC IT Services, Kolkata would be able to take up evaluation only for general purpose IT products and there should be more labs in public/ private sectors in other areas of technology."

1.56 Further, when asked about the agency which is responsible for finding out and implementing global securities best practices in IT in our country, the Department, in their written reply, stated as under:-

"In India, Bureau of Indian Standards (BIS) is mandated with the task of formulating Indian standards on range of topics including IT. Accordingly, BIS has published IS/ ISO/ IEC 27000 series of standards on Information Security Management. These standards are based on International series of standards on the same subject and contain information security management best practices.

Section 43 A of the Information Technology Act 2000 provides for implementing and maintaining reasonable security practice and procedures by a body corporate processing, dealing or handling any sensitive personal data or information. In this connection, rules for Section 43A recognize implementation of security best practices as per ISO 27001 as adequate for the purposes of compliance with the provision of the Act.

Data Security Council of India (DSCI), an industry association is also engaged in compilation of Best Practices, their implementation and audit of the same. CERT-In has also empanelled Security Auditors that provides services relating to audit of Best Practices."

## VI. Upcoming technology *viz*. cloud computing, etc.

1.57 During the course of examination of Demands for Grants (2012-13), the Department had informed that they were planning to use the new technology i.e. Cloud Computing for e-Governance Programmes and storing of its data. The Standing Committee on Information Technology in their Report on Demands for Grants (2012-13) had recommended the Department for evaluating the security and technological challenges associated with cloud computing. It has been noted that one of the strategies outlined for NCSP-2013 is securing e-Governance Services.

1.58 On being enquired by the Committee about the action taken by the Department for securing all the e-Governance Programme and data of Government organisations

and removing the risk of data theft/ disruption particularly emerging from the implementation of new /upcoming technology. The Department stated that State Data Centres (SDC), State Wide Area Network (SWAN) and State Delivery Gateways (SSDG) are the three main components of e-Governance Programme. It has taken following measures to protect the Infrastructure and data from disruption/theft.

- It is mandatory for all State Data Centres to be ISO 27001 (International standard for Information Security Management System) certified within six months of commencement of operations.
- Adequate physical security mechanisms are in place to protect the physical infrastructure from disruptions. The physical infrastructure is protected from unauthorised access by use of access control mechanism like biometric access controls, guards, and visitor access control measures. The physical infrastructure is protected from vagaries of nature by use of environmental control measures.
- Technologies like firewall, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) have been deployed to protect the government network from cyber attack.
- Applications of the government departments are tested for security by agencies empanelled by Cert-In like Standardization Testing and Quality Control (STQC). Security certificate is obtained before the applications are hosted in the State Data Centre.
- In all e-Governance schemes, there is a provision for third party audit of the state data centres (SDC) for overseeing the SDCs' operations and management control processes besides auditing their security processes. STQC in turn, audits the third party auditors on quarterly basis.
- DeitY has notified and published a security assurance framework (e-SAFE ) to guide State Governments and Government Departments in implementation of security controls.

1.59 The Department further informed that as far as new technology like cloud computing is concerned, Government of India has recently published “GI Cloud Strategy and implementation Roadmap Reports” as a part of the Cloud initiative. As a part of this initiative, DeitY shall prescribe the standards and guidelines on security addressing the various challenges and risks.

1.60 As per the Government of Indian’s GI cloud (Meghraj) Strategic Direction Paper, GI-Cloud Computing involves following risks:

1. Risk of compromise of confidential information and intellectual property (IP).
2. Risk of inappropriate access to personal and confidential information.
3. Appropriate privacy and security measures need to be in place.

1.61 When asked as to how safe the ‘e-Governance’ projects are from cyber security breaches and whether there been instances of cyber security breaches in the past, the Department informed that adequate security measures are in place to protect the e-Governance programme and data from theft and disruption. No specific data is maintained regarding instances of security breaches in the past.

## CHAPTER-IV

## CYBER CRIME PREVENTION: ROLE OF CERT-IN & OTHER ORGANISATIONS/ DEPARTMENTS

### I. Role of Cert-In

1.62 The Department has informed that CERT-In is the national nodal agency set up under Section 70B of the Information Technology Act, 2000 to respond to computer security incidents as and when they occur. CERT-In creates awareness on security issues through dissemination of information on its website (http://www.cert-in.org.in) and operates 24X7 Incident Response Help Desk. It provides Incident Prevention and Response services as well as Security Quality Management Services.

1.63 When asked as to what extent CERT-In has been able to prevent cyber- threats, the Department in their written reply stated that CERT-In performs Computer Security Incident Response and prevention and provides Security Quality Management Services. Specific activities of CERT-In in preventing cyber threats are:

- Coordinate responses to security incidents and major events
- Issue advisories and timely advice regarding imminent threats
- Work with industry and security experts to identify solution to security problems
- Analyze product vulnerabilities and malicious code
- Analysis of web defacements on regular basis
- Analysis of open proxy servers on regular basis to mitigate spam and anonymization threats
- Helping organisations in profiling the network and the attacking systems
- Interact with vendors and others at large to provide effective and timely solutions for incident resolution and investigation
- Conduct training on specialized topics of cyber security
- Develop security guidelines on major platforms
- Collaborating with Industry and overseas CERTs for effective incident resolution

1.64 In addition CERT-In has taken following initiatives for proactive cyber threat prevention

- A “Crisis Management Plan for countering cyber attacks and cyber terrorism” has been prepared and circulated for implementation by all Ministries/Departments of Central Government, State Government and all their organizations and critical sectors.

- Empanelment of security auditors to conduct security audit, vulnerability assessment and penetration testing of Indian organizations
- CERT-In has been carrying out cyber security mock drills on a periodic basis for assessing the preparedness of critical sector organizations in dealing with cyber crisis. Cyber security drill is a confidence building and learning exercise based on simulated cyber security incident scenarios that resemble occurrence of a cyber security crisis.

1.65 On the basis of these guiding principles, following co-ordination and oversight structure is proposed by the Department:-

- "There should be a permanent Joint Working Group (JWG) under the aegis of the National Security Council Secretariat (NSCS) with representatives from Government as well as Private Sector.
- This JWG will act as an advisory body and co-ordinate Public-Private Partnership (PPP) on cyber security.
- A Joint Committee on International Cooperation and Advocacy (JCICA) will be set up as a permanent advisory committee of the JWG in promoting India's national interests at various international fora on cyber security issues.
- The composition of both JWG and JCICA will be finalized in consultation with industry associations.
- The private sector will set up Information Sharing & Analysis Centres (ISACs) in various sectors and cooperate with the sectoral CERTs at the operational level."

## II. Role of other Organisations/Departments

1.66 On being asked about the various organisations that are involved in securing India's cyber space, the Department, in their written reply, submitted as under:-

"Ministry of Defence (MoD)

Ministry of Defence is the nodal agency for cyber security incident response with respect to Defence sector. MoD, IDS (DIARA), formed under the aegis of Headquarters, Integrated Defence Staff, is the nodal tri-Services agency at the national level to effectively deal with all aspects of Information Assurance and operations. It has also formed the Defence CERT where primary function is to coordinate the activities of services/MoD CERTs. It works in close association with CERT-In to ensure perpetual availability of Defence networks.

Ministry of Home Affairs and Intelligence Bureau (IB)

Ministry of Home Affairs reviews the overall preparedness of respective Ministries and critical sector organisations under these Ministries with respect to physical security and crisis management. Intelligence Bureau issues overall guidelines to Ministries and critical sectors in respect of security matters in general. IB also plays nodal role and sensitises the administrative departments and critical sector organisations on latest threats and issues security guidelines from time to time to secure IT and physical infrastructure. The respective Central Administrative Ministries/Departments and their critical sector organisations shall implement these guidelines for beefing up/strengthening the security measures of their infrastructure. IB, CERT-In and NTRO will mutually exchange information to support activities of each other.

Department of Telecommunications

Department of Telecommunications (DoT) will co-ordinate with all ISPs and service providers with respect to cyber security incidents and response actions as deemed necessary by CERT-In, NTRO, MoD, IB and other Government Agencies. DoT will provide guidelines regarding roles and responsibilities of Private Service Providers and ensure that these Service Providers install GIS based system to track the critical optical fibre networks and arrangements of alternate routing in case of physical attacks on these networks.

National Disaster Management Authority (NDMA)

NDMA has been mandated to develop pro-active, multi-disaster and technology-driven strategy for disaster management through collective efforts of all Government Agencies and Non-Governmental Organisations. NDMA will facilitate and make available their resources and reach to the respective Administrative Ministry to support response and mitigation actions for countering cyber attacks and cyber terrorism.

National Technical Research Organisation (NTRO)

NTRO provides all technical support to Intelligence and security agencies to keep watch and imminent cyber threats. It is also a designated agency to protect Critical Information Infrastructure in the country from cyber threats. They would prepare threat assessment reports and facilitate sharing of such information and analysis among members of its constituency with a view to protecting these agencies' ability to collect, analyze and disseminate intelligence. NTRO would share intelligence information and interact with CERT-In and also with other incident response organisations and provide advance information on potential threats.

National Critical Information Infrastructure Protection Centre (NCIIPC)

NCIIPC is a designated agency to protect the critical information infrastructure in the country. It gathers intelligence and keeps a watch on emerging and imminent cyber threats in strategic sectors including National Defence. It would prepare threat assessment reports and facilitate sharing of such information and analysis among members of the Intelligence, Defence and Law enforcement agencies with a view to protecting these agencies' ability to collect, analyze and disseminate intelligence. NCIIPC would interact with other incident response organizations including CERT-In, enabling such organizations to leverage the Intelligence agencies' analytical capabilities for providing advanced information of potential threats.

Research and Analysis Wing (R&AW)

Research and Analysis Wing (R&AW), monitors, gathers intelligence and keeps a watch on emerging and imminent threats from external sources. MHA, IB, R&AW, CERT-In and NTRO will mutually exchange information about cyber threats and hostile activities of individuals, groups and agencies operating from outside the country.

Indian Computer Emergency Response Team (CERT-In)

CERT-In monitors Indian cyberspace and coordinates alerts and warning of imminent attacks and detection of malicious attacks among public and private cyber users and organisations in the country. It maintains 24x7 operations centre and has working relations/collaborations and contacts with CERTs all over the world; and Sectoral CERTs, public, private, academia, Internet Service Providers and vendors of Information Technology products in the country. It would work with Central Ministries and monitors cyber incidents on continuing basis throughout the extent of incident and would analyse and disseminate information and guidelines. The primary constituency of CERT-In would be all organisations other than Defence, Space, Atomic Energy, Law Enforcement and security agencies and their critical infrastructure."

1.67 When asked as to whether the Department is satisfied with the role and functioning of different organisations/Departments involved in securing India's cyber space, the Department, in their written reply stated as under:-

"Various organisations in the country have been engaged in the task of dealing with the issues and different aspects related to cyber security. In order to address effectively the issue of overlapping responsibilities and enhancing coordination between the stakeholder agencies in the country, Government has approved a framework for enhancing Cyber Security which envisages a multi-layered approach for ensuring defence in-depth and allocates the responsibility for overall cyber security among the stakeholder organizations in the country.

The National Security Council Secretariat is tasked to co-ordinate, oversee and ensure compliance of cyber security policies."

1.68 Further, on being asked about the frequency and the level of interaction with the State Governments/other agencies and Ministries so as to tackle cyber cases the Department, in their written reply, submitted as under:-

"CERT-In regularly interacts and works with State Governments and Central Ministries and monitors cyber incidents on continuing basis throughout the extent of incident and would analyse and disseminate information and guidelines.

CERT-In assists user entities to understand the concept of Crisis Management Plan (CMP) and its implementation by conducting workshops on CMP and IT security best practices for Sectors/ States/ Ministries/ Departments/ Organisations on-site or at CERT-In facility. Till date, 20 CMP Workshops have been conducted by CERT-In for various entities.

To enable organisations to assess their preparedness in dealing with cyber crisis, CERT-In is conducting Cyber Security drills of different complexities with various key organisations. So far, 7 drills have been conducted involving more than 110 organizations from Defence, Space, Atomic Energy, Telecommunications (ISPs), Finance, Power, Petroleum & Natural Gas, Transportation (Railways & Civil Aviation) and IT/ ITeS/ BPO sectors."

1.69 Public private partnership is very important to address the issue of cyber security. In this context, the Committee desired to know whether the Department has taken any initiative to have public private partnership. To this, the Department in their written reply stated that one of the primary challenges faced by both Government as well as Industry is to curb the cyber threat at the earliest and this cannot be achieved in isolation by either Government or Industry alone. It requires collaboration and coordinated efforts of all the organisations involved in securing the country's cyber space.

1.70 According to the Department after a discussion with representatives of the private sector on their role in enhancing cyber security, it was decided to set up a Joint Working Group (JWG), under the chairpersonship of the Deputy National Security Advisor, to work out the details of the Roadmap for cyber security cooperation that needed to be evolved. This JWG included representatives of both Government and private sector. The JWG constituted five Sub-Groups to flesh out the details of such engagement. These five Sub-Groups submitted their reports to the JWG on 16$^{th}$ August, 2012, which thereafter finalized its recommendations. The JWG has identified the following guiding principles and objectives that would underpin the public-private partnership (PPP) in cyber security:

"a) Given the diverse stakeholders in cyber security, institutional mechanisms should be set up to promote convergence of efforts both in public and private domains;
b) Use existing institutions and organizations to the extent possible in both private sector and government and create new institutions were required to enhance cyber security;
c) Set up a permanent mechanism for private public partnership;
d) Identify bodies that can play a wider role in funding and implementation in the public and private sector;
e) Identify areas where both private and public sector can build capacities for cyber security;
f) Put in place appropriate policy and legal frameworks to ensure compliance with cyber security efforts;
g) Promote active PPP cooperation in international forums and in formulating India's position on global cyber security policies;
h) Establish India as a global hub of development of cyber security products, services and manpower; and
i) Promote indigenization and work on joint R&D projects to meet the cyber security needs of the country."

## III. Memorandum of Understandings (MOUs) and International treaties to secure Cyber Space

1.71 In a globalised economy, a focused approach to international relations is vital particularly with regard to the cyber space which by its very nature is borderless and anonymous.

1.72 As per the Annual Report (2012-13) of DeitY, in order to promote international cooperation in the emerging and frontier areas of information technology, explore ways to enhance investment and address regulatory mechanism, the Department has taken various collaborative efforts and has geared up to courage sustainable development and strengthening partnerships with other countries.

1.73 In this context, the Committee desired to know the details of MoUs that India has signed so far with various other countries. To this the Department in their written reply stated that Indian Computer Emergency Response Team (CERT-In) enters into international cyber security cooperation arrangements with organizations engaged in similar activities, in the form of Memorandum of Understanding (MoU), to enhance its operational readiness. At present such MoUs have been entered with (i) Computer Emergency Response Team, US (US-CERT), (ii) Japanese Computer Emergency Response Team Coordination Centre (JP-CERT/CC), (iii) National Cyber Security Centre (NCSC), South Korea, (iv) Computer Emergency Response Team, Mauritius (CERT Mauritius) & (v) Computer Emergency Response Team, Kazakhstan (CERT Kazakhstan). Besides,

Government of Finland and Government of India have also signed a MoU on cooperation in the area of cyber security.

1.74 During the year 2012-13, the Department has also signed a MoU with Canada in ICT and Electronics sector. On being asked about the plans envisaged to increase the number of MoUs, the Department, in their written reply, submitted as under:-

> "The Department with the active assistance of Ministry of External Affairs is having engagement dialogue with several countries such as Malaysia, Israel, Egypt, Canada, Brazil that are willing to cooperate and share information with regard to cyber security incidents and vulnerabilities in IT products and systems."

1.75 Highlighting on aspects of co-operation at international level in tackling with new forms of cyber crime such as Botnet, the Secretary submitted during evidence as under:

> "we need to have an international dialogue in different forums for creating a global cyber jurisprudence separately. Our Ministry has already articulated that, how to handle such situations, we need to have a dialogue. A new cyber jurisprudence has to come up. New international court for cyber jurisprudence has to come up."

## CHAPTER-V

## PREPAREDNESS AND POLICY INITIATIVES

1.76 Keeping in view the security risks and vulnerabilities of the internet/computer run systems, the Committee desired to know about the level of preparedness of the Government, if the systems like defence establishments, hospitals, transportation, Banks, Government organisations, etc., are hijacked or manipulated through cyber attacks. To this, the Department, in their written reply, submitted that the Government has taken several actions to improve the alertness of the Government and other critical sector organisations. As part of the 'Crisis Management Plan' (CMP) for countering cyber attacks and cyber terrorism" all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors have been mandated to continuously assess the posture of their IT systems and networks. The CMP mandates following specific steps:

- Nominate Chief Information Security Officers to co-ordinate the security related issues/implementation within the organisation as well as coordination and interface with CERT-In
- Security devices may be installed at all levels. Servers, Local Area Network (LAN) and Wide Area Network (WAN) infrastructure should be secured by installing appropriate perimeter security devices such as firewalls, Intrusion Prevention System and anti-virus system. These security mechanisms should include appropriate devices and methods to log and monitor the events to detect network scanning, probing and Reconnaissance attempts on the IT infrastructure. These attempts should be regularly reviewed and analysed for initiating necessary preventive measures.
- Deployment of network traffic scanning technique to improve the visibility into the state of the network and identifying deviations from baselines that may indicate abnormal or suspicious behaviour.

1.77 The Department also informed that in order to improve the alertness at the national level the Department has advised organizations to report to CERT-In within one hour of occurrence of the incident or noticing of cyber security incidents such as:-

- Targeted scanning/probing of critical networks/systems
- Compromise of critical systems/information
- Unauthorised access of IT systems/data
- Defacement of website or intrusion into a website and unauthorised changes such as inserting malicious code, links to external websites etc.
- Malicious code attacks such as spreading of virus/ worm/ Trojan/ Botnets/ Spyware
- Attacks on servers such as Database, Mail and DNS and network devices such as Routers

- Identity Theft, spoofing and phishing attacks
- Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks
- Attacks on Critical infrastructure, SCADA Systems and Wireless networks
- Attacks on Applications such as E-Governance, E-Commerce etc.

1.78 Elaborating on the preparedness to deal with cyber crisis, the Department, in their written reply, submitted as under:-

> "Cyber security requires a coherent conceptualization, clear vision of purpose and objectives and a time bound plan of action. Formulation of a national approach involves using elements of national power including political, economic, military and technological capabilities during peace and war to achieve national objectives. Towards this end, the Department of Electronics & Information Technology (DeitY) formulated a Crisis Management Plan (CMP) for Countering Cyber-attacks and Cyber-terrorism in 2010 that has been periodically updated. The current version for the year 2013 is ready for release. The purpose of the CMP is to establish the strategic framework and actions to prepare for, respond to and begin to coordinate recovery from a cyber incident. It is independent of computer hardware, operating system and applications."

## I. Cyber Crisis Management Plan (CCMP)

1.79 On the Cyber Crisis Management Plan (CCMP) of India, the Department, in their written reply, submitted as under:-

> "Based on the decisions of the committee of Secretaries chaired by Cabinet Secretary, CERT-In has developed the National Crisis Management Plan (NCMP) for Countering Cyber Attacks and Cyber Terrorism. The Crisis Management Plan is being revised on annual basis in line with the decisions taken during the meeting of National Crisis Management Committee (NCMC) on Cyber Security under the chairmanship of cabinet Secretary.

1.80 The salient features of Cyber Crisis Management Plan (CCMP) as furnished by the Department are as follows :-

- Outlines a framework for dealing with cyber related incidents for a coordinated, multi disciplinary and broad based approach for rapid identification, information exchange, swift response and remedial actions to mitigate and recover from malicious cyber related incidents impacting critical national processes.
- Includes both proactive and reactive approach to deal with cyber crisis situations.
- Guide actions to prepare for, respond to, and begin to coordinate recovery to cyber incident.
- To ensure that interruption or manipulations of critical function/services in critical sector organisation are brief, infrequent and manageable and cause least possible damage.

- To assist organisations to put in place mechanism to effectively deal with cyber security crisis and be able to pinpoint responsibilities and accountabilities.

1.81 On being asked as to how the Cyber Crisis Management Plan is proposed to be implemented, the Department stated that the following action is being taken for implementing the Plan:-

- National CMP document developed by DeitY is circulated to all the Ministries, States and Sectors with guidelines for CMP development and implementation.
- Instructions along with guidelines for development of CMP to all sectors/states/ministries/departments are coordinated by NCMC and CERT-In.
- To assist States/Ministries/Departments/ Organisations in preparation of CMP, Sectoral CMP template is provided to them.
- CMP developed by various Sectors/ States/ Ministries/ Departments/ Organisations are reviewed by CERT-In and appropriate suggestions are provided to improve the CMP.
- CERT-In assist entities to understand the concept of CMP and its implementation by conducting workshops on CMP and IT security best practices for Sectors/ States/ Ministries/ Departments/ Organisations on-site or in CERT-In facility. Till date, 20 CMP Workshops have been conducted by CERT-In for various entities.
- To enable organisations to assess their preparedness in dealing with cyber crisis, CERT-In is conducting Cyber Security drills of different complexities with various key organisations. So far, 7 drills have been conducted involving more than 110 organizations from Defence, Space, Atomic Energy, Telecommunications (ISPs), Finance, Power, Petroleum & Natural Gas, Transportation (Railways & Civil Aviation) and IT/ ITeS/ BPO sectors.

## II. National Cyber Security Policy, 2013 (NCSP-2013)

1.82 The Department informed that the Government of India had on 08 May 2013 approved a National Cyber Security Policy whose stated mission is "to protect information and information infrastructure in cyber space, 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". It seeks to do so by creating a secure cyber ecosystem and an assurance framework, encouraging open standards, strengthening the regulatory framework, vulnerability management, promotion of research and development in cyber security and enhancing our technical skill sets and human resources.

1.83 The Government also simultaneously approved the Framework for Enhancing Cyber Security which envisages a multi-layered approach for ensuring defense in-depth and allocates the responsibility for overall cyber security among the stakeholder organizations in the country. The National Security Council Secretariat is tasked to co-ordinate, oversee and ensure compliance of cyber security policies.

1.84 Regarding the aims, objectives and background of the Policy the Department , in their written reply, submitted as under:-

"The National Cyber Security Policy required consultation with all relevant stakeholders, user entities and public. The policy document aimed at creating a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country. Accordingly, DeitY had prepared a draft discussion document on "National Cyber Security Policy" for public consultation in the month of March, 2011. The draft discussion document was widely circulated among stakeholders and also put on DeitY website for public consultation and seeking comments/suggestions by 15th May, 2011. In addition, comments on the draft document were also sought from all the leading industries associations. The comments were received from more than 50 sources including Central Government/ Ministries/ Departments, State Governments, International Agencies, Industries and Individuals. The comments received from various sources were analysed and final version of National Cyber Security Policy was launched in 2013 after appropriate modifications in the draft of National Cyber Security Policy document based on suggestions received.

This policy aims at facilitating creation of secure computing environment and enabling adequate trust and confidence in electronic transactions and also guiding stakeholders' actions for protection of cyber space.

The National Cyber Security Policy document outlines a road-map to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country.

The policy recognises the need for objectives and strategies that need to be adopted both at the national level as well as international level.

The objectives and strategies outlined in the National Cyber Security Policy together serve as a means to:

i. Articulate our concerns, understanding, priorities for action as well as directed efforts.
ii. Provide confidence and reasonable assurance to all stakeholders in the country (Government, business, industry and general public) and global community, about the safety, resiliency and security of cyber space.
iii. Adopt a suitable posturing that can signal our resolve to make determined efforts to effectively monitor, deter & deal with cyber crime and cyber attacks.

1.85 On being asked as to by what time the Rules/Guidelines for NCSP-2013 would be in place, the Department , in their written reply, submitted as under:-

> "The National Cyber Security Policy provides a roadmap to create a framework for comprehensive, collaborative and collective response to deal with issues of cyber security at all levels within the country. The policy is to be implemented to set up action oriented programmes. Some of the programmes will be implemented by Government and some of which will be implemented by the private sector and other stakeholders. Government is in the process of preparing individual schemes which are to be implemented by the Government. The Joint Working Group set up under the aegis of National Security Council Secretariat (NSCS) is also engaged in drawing a roadmap for taking action arising out of the policy in a public-private mode. It is our endeavour to obtain major programmes at the earliest and implement such major programmes in the next one year."

1.86 The Department has informed that out of 47 objectives outlined in NCSP-2013, eight areas have been prioritized by the Department which are as under:-

- To designate a National nodal agency to coordinate all matters related to cyber security in the country, with clearly defined roles & responsibilities.
- To create National level system, processes, and mechanism 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.
- To operate a 24X7 National Critical Infrastructure Protection Center (NCIIPC) to function as the nodal agency for critical information infrastructure protection in the country.
- 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)
- To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices -Crypto module evaluation
- To create and maintain testing infrastructure and facilities for IT security product evaluation and compliance verification as per global standards and practices - CC test/ evaluation
- To foster education and training programs both in formal and informal sectors to support the Nation's cyber security needs and build capacity
- To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security.

1.87 When asked about the existence of any model/guideline that can be adopted by various stakeholders involved in securing cyber space, the Department , in their written

reply, submitted that various guidelines/ documents in existence which can be adopted by various entities. These are as under:

- Cyber Security Policies for Government of India published by DeitY.
- Standard Operating procedures for Cyber Security Policies for Government of India Published by DeitY.
- Set of investigation manuals with procedures for Search, Seizure Analysis and Presentation of digital evidence in courts.
- Crisis Management Plan for countering cyber attacks and cyber terrorism published by DeitY.
- Cyber security guidelines published by CERT-In on issues such as hardening of systems etc.
- Guidelines published by National Informatics Centre (NIC) from time to time such as web hosting etc.
- Guidelines published by CERT-In on IT security audit related issues."

1.88 Elaborating on the statutory framework, nodal agency, etc., for implementing NCSP-2013, the Department, in their written reply, submitted as under:-

> "Necessary steps towards designating the national nodal agency have already been initiated by the Government..x..x..x. The National Security Council Secretariat is tasked to co-ordinate, oversee the implementation of cyber security policy. x..x..x.. Government has initiated steps towards establishment of National Critical Information Infrastructure Protection Centre (NCIIPC). National Technical Research Organization (NTRO) has been tasked with the responsibility of creation and functioning of NCIIPC. x..x..x.. DeitY has already initiated steps to identify the follow up actions as well as agencies responsible and timelines for such actions. The actions of DeitY are in line with the Government approved Framework for Enhancing Cyber Security which envisages a multi-layered approach for ensuring defense in-depth and allocates the responsibility for overall cyber security."

## III. Information Technology Act, 2000 and Cyber Security

1.89 On being enquired about the details of all the Acts/legislations/regulatory framework that are currently in vogue to deal with cyber crime and cyber attacks, the Department, in their written reply, stated that Sections 43A, 66 A, 67, 69 B, 70 (1), 70 (4), 70-B, 72 A, 79 and 84 A, in the Information Technology Act, 2000 (IT Act) deal with cyber crime and cyber attacks.

1.90 Asked as to how far the various sections of IT Act, 2000 as amended in 2008 have been successful in tackling the issues of cyber crime/cyber security, the Department in their written reply, stated that the various provisions in the IT Act that make the actions effective in dealing with cyber crime and cyber attacks are as under:

- "Indian Computer Emergency Response Team (CERT-In) as the national agency for incident response - As part of provisions contained in 70-B of the IT Act, CERT-In is the National Agency to coordinate all security related matters and emergency response in the country.
- Collection and sharing of information related to cyber incidents for effective proactive/reactive actions by CERT-In and investigative actions by law enforcement agencies - Section 70-B and Section 69-B of the IT Act provide for seeking information and collection of data/information related to cyber incidents. These provisions help in security incidents prevention and prediction.
- Prescription of security best practices and guidelines to prevent occurrence and recurrence of security incidents - Section 70-B and Section 43 A of the IT Act contain provisions for prescribing security best practices for compliance by corporate and critical sector organizations.
- Ensuring implementation of security best practices and compliance to the same by organizations in critical sector - As part of security incidents prevention activities under Section 70-B of the IT Act, DIT is reviewing periodically compliance to security best practices by Govt. and critical sector organizations.
- Protection of Critical Information Infrastructure to safeguard the critical ICT assets - Section 70 (1) allows for declaration of an ICT asset as a protected system if it directly or indirectly affects the facility of Critical Information Infrastructure. Section 70 (4) allows for prescription information security best practices and procedures for such protected system. Govt. has initiated steps to notify a national nodal agency for protecting critical information infrastructure in the country.
- Comprehensive plan for countering cyber attacks and cyber terrorism - As part of provisions contained in 70-B of the IT Act, CERT-In is the National Nodal Agency to coordinate all security related matters and emergency response in the country. Accordingly, it has created a comprehensive Crisis Management Plan for countering cyber attacks and cyber terrorism. This plan has been approved by the National Crisis Management Committee chaired by Cabinet Secretary for implementation across the country. This Crisis Management Plan aims at - Enhancement of ability to withstand and resist cyber attacks and improving the security posture of critical sector organizations. This CMP has provisions for conducting cyber security drills in the form of simulated cyber attacks to verify the implementation of crisis management plan and cyber security management.
- Effective deterrence provisions in terms of compensation and punishment to deal with cyber crime such as spam, abusive mails, cyber terrorism and child pornography, criminal act using computer etc. - Section 43-A of the IT Act contains provisions to prescribe compliance requirements for data security and privacy protection and compensation for non compliance. Sections 43, 66, 66A, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 72 and 72A of

the IT Act deal with host of cyber crime activities with adequate deterrent punishment.

- Breach of privacy – Section 72 A provides for adequate punishment for disclosure of information in breach of lawful contract.
- Liability of intermediaries – Section 79 covers instances of liabilities of intermediaries and requirement for due diligence on the part of intermediaries.
- Modes of encryption – Section 84 A allows for prescription of suitable modes or methods of encryption for promotion of e-commerce and e-governance in the country.
- Rules for cyber cafes – Separate rules for cyber cafes help in regulating the malicious activities that can be carried out in cyber cafes and provide a mechanism to prevent and deal with instances of cyber crime in an effective manner."

1.91 On the issue of adequacy of the existing legal framework for dealing with the cyber-crimes, the Department, in their written reply, stated that IT Act, 2000 addresses all aspects related to cyber crimes in a comprehensive manner with adequate deterrent provisions. In addition, the National Cyber Security Policy-2013 has provisions to enable development of a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space.

1.92 Asked as to whether there is a need for amending Information Technology Act, 2008 in the emerging scenario, the Department in their written reply stated as under:-

> "At present, the IT Act 2000 addresses all aspects related to cyber space in a comprehensive manner with adequate compliance and deterrent provisions. In addition, the National Cyber Security Policy 2013 has provisions to enable development of a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space."

1.93 Even with respect to the National Cyber Security Policy, the Department stated that at present no need is felt to amend the Information Technology Act to address National Cyber Security Policy. However, they also stated that since it is a dynamic area, as and when needed, IT Act will be amended.

1.94 On the issue of overall preparedness, the Secretary, during evidence, enumerated as under:-

> "….x..x..x.. CERT itself has given comprehensive policies to all the organisations not only in the Government but also outside. So, security guidelines and principles have been documented and sent. x…x…x… Crisis Management Plan is one more instance to indicate our readiness. x…x…x…Third is the policy (NCSP-2013) itself is quite an important achievement because it is one of the few

countries, as we submitted at the last sitting of this Committee, that has got such a widespread policy on cyber security. Yes, we need to translate it into certain schemes and we will be doing that.

One more important aspect is,…x…x…x… that a draft has been prepared for *comprehensive e-mail policy for the Government of India* …x…x…x….This is a very comprehensive document. So far we have four lakh users in the Government using e-mail and several instructions have been given from time to time but there is no single compendium or a policy to ensure that e-mail is properly used or not leaving loopholes for outsiders for either stealing the information, etc. So, it is a comprehensive policy covering not only the Central Government but also the State Governments which use the NIC mail server because mail is one of the important ways through which all the sensitive information, if it is hacked, of the Government can be accessed and misused by the outside elements. So, we are on the verge of it and the draft is ready. It is a question of processing time and at the earliest we will be releasing this policy and enforcing it. This is one more good measure in which we are going forward.

On the aspect of usage of internet, especially in the Government place, when a private citizen uses internet in his or her own way we cannot say that he or she will use the internet but using the Government networks you are exposing our own system to the outside world. Therefore, necessary precaution, especially the security point of view precaution has to be taken. As a supplement to the earlier policy we have brought out this policy which is called the *'Acceptable Internet Usage Policy',* for what purposes you can use internet and for what purposes you cannot, etc. This will bring out this policy together with e-mail and both will be processed very soon and strengthen our own defence considerably because these are the weak points for the Government. So, we are going to come out soon. My estimate would be that it should be about eight to ten week's time because inter-ministerial consideration has to be done before we issue policy because it should be applicable to all Ministries…xxx……..xxx…….xxx……xxx……xxx… there may be some security issues arising out of cloud. We cannot shun away from this upcoming technology because it brings a lot of benefits. So we have come out with a kind of information, two sets of policies which I will also pass on to the hon. Committee. One is called the Government of India's strategic direction paper on cloud which is also called 'Meghraj' indicating Government cloud, how Government can use the cloud of its own. It is just published a few weeks back and I am passing. So this also has an element of security built into this. What precautions need to be taken, it is also inbuilt into this. Along with it, it is a roadmap which gives the more clear dimension to the timelines, how we want to implement and so on. So this is also I would like to just mention because one of the questions contained about what is your response to cloud. So we are ready with our own this thing. We are already implementing. The first phase of it will be implemented by the end of September in Delhi itself; about 100 project in we are using for the Government purposes with all security. So what we have told is that in some of the countries like Namibia, they came up with

the policy of cloud first. But then there were also concerns about the security. So, what we have re-designated that was security first, cloud next is the kind of philosophy which we want to push this. Whatever security we wanted out, look at security first. And then use it."

## CHAPTER-VI

## CYBER SECURITY AND RIGHT TO PRIVACY

1.95 As per the background note furnished on the subject, balancing cyber security, cyber crime and right to privacy is an extremely complex task due to the nature of the cyber space which is borderless. It requires the maturity and competence of seasoned professionals who have skills in multiple disciplines at the same time, namely technical (deep understanding of ICT and cyber security), protection (technical, process and administrative controls), legal and regulatory, constitutional, diplomacy, communication skills, public policy, psychology and economics to name a few.

1.96 Regarding measures that are in place for balancing privacy concerns while dealing with cyber threats, the Department, in the background note, submitted as under :-

> "The Information Technology Act 2000 contains adequate provisions to deal with various cyber related offenses as well as protection of privacy of individuals. The following is a brief on such provisions in the Act:
> - Section 43 and section 66 of the Information Technology Act, 2000 provides penalty and stringent punishment for hacking of website.
> - Section 43A of the Information Technology Act, 2000 provides compensation to the affected person for failure to protect data
> - The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 notified on 11th April, 2013 under section 43A of the Information Technology Act defines the sensitive personal data and reasonable security practices and procedures. The Rules require body corporate to provide policy for privacy and disclosure of information (Rule 4), obtain consent of user for collection of information (Rule 5), prior permission required from provider of information before disclosure of sensitive personal information (Rule 6)
> - Section 72 of the Act provides penalty for breach of confidentiality and privacy
> - Section 72A of the Act provides punishment for disclosure of information in breach of lawful contract."

1.97 In reply to an unstarred question (No.1969) replied in Lok Sabha on 5th December, 2012, as to whether the Government proposes to introduce relevant law/rules for unauthorized sharing of personal information and its disclosure and make it as a cognizable offence, the Minister of State for Communications and Information Technology stated as under:-

> "Section 43A of the Information Technology Act, 2000 and Rules notified there under establishes a legal framework for data privacy protection in India. It mandates body corporate to implement reasonable security practices, framework for mode of collection, transfer and disclosure of sensitive personal data or information. Further, section 66C and 72A of the Information

Technology Act, 2000 provides for punishment and penalty for identity theft and breach of confidentiality and privacy respectively."

1.98 When the Committee desired to know the adequacy of the existing provisions in the law so as to address the issue of right to privacy, the Department in their written reply submitted as under:-

"xxx…xxx...xxx…Department of Personnel and Training is engaged in evolving legislation to address concerns of privacy, in general in country. The proposed legislation together with section 43A of the Information Technology Act, 2000 is expected to address all concerns of privacy in the cyberspace and in general."

1.99 Further, on being asked whether any study has been conducted by the Government to estimate the extent of privacy breach and type of breaches happening due to cyber-crime, the Department, in their written reply, submitted as under:-

"Government has not conducted any study to estimate the extent of privacy breach and type of privacy breach happening due to cyber crime. However, Data Security Council of India (DSCI), an industry association of NASSCOM has been engaged in conducting such a study focusing on privacy breach.

1.100Elaborating on the issue of cyber security and Right to privacy, the Secretary, DeitY, during evidence, submitted as under:-

"Regarding personal information and the right to privacy already, the IT Act, section 43A and 72A has got provisions to safeguard the personal information in the sense that if any organisation which is in possession of the private personal information of the individuals, reveals to other without consent of the individual, it is a punishable offence under the IT Act with imprisonment of up to three years. If any such case comes to the notice, immediately cognizance can be taken. It is already provided under section 72A. So, the companies are obliged to keep confidentiality of the personal information of individuals. Apart from the legal provisions, more workable and more operative thing is the fact that India is one of the top most countries in the world in terms of business processes outsourcing (BPO) operations.

So, a large number of IT companies in this country are receiving personal data of people from all over the world and they are processing that data as per their client's requirement without any major concerns or complaints. It is a question of survival also. If this information is traded by these companies, then obviously the reputation of the company as well as the country will be on stake. Hence, there is also available a commercial safeguard, a professional safeguard apart from the legal safeguard. That I would say regarding the privacy.

The third point is the fact that the Government of India is considering the enactment of a privacy law in the country. At present, it is at a draft stage. It is being piloted by the Department of Personnel for all the Ministries put together. So, it has substantive provisions relating to the personal data pertaining to the

residents of India. How the privacy of such information should be and shall be protected and what are the consequences if it is not protected – the provisions in this regard are also going to be enlarged, which are available to some extent in Section 43 of the IT Act. ”

1.101The Director- General, CERT-In, during evidence, added as under:-

“With regard to right to privacy, ..x.x.x... Section 43A mandates the body corporates or the service providers to implement the best practices to protect the data leakage from their servers. As part of the Act we have defined what reasonable security practices the body corporate will have to implement. In the rules we have defined ‘sensitive personal data information’. There are about ten parameters. There are credit card numbers, health details, financial details, biometric data, password, etc. Those ten parameters have defined.

As regard to personal information, ..x.x.x.. DoPT is evolving a general framework for the privacy law. So, personal information is a little wider aspect which may not come under the purview of Department of Electronics and Information Technology because it contains personal data which is not part of DeitY. We can be concerned only with the digital data. So, all those parameters which are seen as part of digital data, as part of the mandate of this Ministry, have been addressed in rules under Section 43A of the IT Act.”

The reasonable best practices have been notified on 11th April, 2011 and many of the body corporates are implementing best practices. In case there is a leakage of data the victim again can file compensation or claim damages and the lower courts can award compensation up to Rs.5 crore and for the higher compensation the case can go to the higher courts or other competent courts there. That is Section 43. So, Section 43A and the rules published under that Section cover the entire privacy in case of digital data. These are being followed by UIDAI also and other organisations.

The entire Section 43A is based on self regulation. Companies will have to implement those best practices, not only the notified best practices but if a cluster of organisations want to have their own best practices suitable for their business, they can get the best practices approved by the Department and they can implement those, notify on their website that these are the best practices they will follow and those practices can be audited by independent auditors, either those 44 or others. So, it is a complete process of self regulation. Government does not want to come into the picture.”

1.102In the context of privacy of data, the Committee desired to know the Department’s stand on the issue of surveillance by US and interception of data sent through e-mails. To this, the Secretary, DeitY, responded during the evidence as under:-

“Sir, about the US surveillance issue, there has been a debate, as you are aware, this morning in the Rajya Sabha itself and the hon. Minister has addressed this issue. He also emphasised that as far as the Government data and Government

mails are concerned, the policy, the copy of which I have given to the Committee earlier, is going to address a large part of it. Hopefully, by the end of this year, if it is implemented, the things will be absolutely safe and secure…x.x.x.x…In the reply, the Hon. Minister also said that we have expressed our serious concern about the reported leakages and in the name of surveillance, the data that has been secured from various private sources, internet resources by the US Government. We have expressed it formally to the Government of the US and also during the Secretary of State's visit a few weeks ago in India, this has been reinforced on a person to person basis. We have been assured that whatever data has been gathered by them for surveillance relates only to the metadata. It has been reiterated and stated at the highest level of the US President that only the metadata has been accessed, which is, the origin of the message and the receiving point, the destination and the route through which it has gone, but not the actual content itself. This has been reiterated by them, but we expressed that any incursion into the content will not be tolerated and is not tolerable from Indian stand and point of view. That has been mentioned very clearly and firmly by our Government."

## CHAPTER-VII

## MONITORING AND GRIEVANCE REDRESSAL MECHANISM

1.103On being asked whether there is a centralized system/cell for monitoring cyber-crime and also at the State level, the Department, in their written reply stated as under:-

> "Law and Order being a State subject, all actions related to crime including cyber crime are dealt with by respective States/UTs and relevant data is being maintained by National Crime Records Bureau (NCRB). Many of the States have set up cyber crime cell which are monitoring such crimes."

1.104When the Committee desired to know the existing grievance redressal mechanism for cyber-crime cases in the country, the Department, in their written reply, submitted that after registering a complaint with the local police stations or cyber crime cells of Law Enforcement agencies, further redressal process of such cases is similar to other crime related cases.

1.105When enquired about the organisation which can be approached by the common man for complaints regarding cyber-crime, the Department stated that the present system involves reporting with the local police stations or cyber crime cells of law enforcement agencies across the country.

### I. Cyber Appellate Tribunal (earlier known as Cyber Regulations Appellate Tribunal)

1.106The Department informed that in accordance with the provision contained under Section 48(1) of the IT Act 2000, the Cyber Regulations Appellate Tribunal (CRAT) was established in October, 2006. As per the IT Act, any person aggrieved by an order made by the Controller of Certifying Authorities or by an Adjudicating Officer under the Act can prefer an appeal before the Cyber Appellate Tribunal (CAT). This Tribunal is headed by a Chairperson who is appointed by the Central Government by notification as provided under Section 49 of the IT Act 2000. Before the amendment of the IT Act in the year 2009, the Tribunal was known as CRAT and the Chairperson was known as the Presiding Officer. Provision has been made in the amended Act for the Tribunal to comprise a Chairperson and such number of other members as the Central Government may notify/appoint. The name of CRAT has also been changed to CAT.

1.107The main objectives of the Cyber Appellate Tribunal are (i) to consider and decide the validity/legal propriety of the orders passed by the Adjudicating Officers and (ii) to spread awareness about the Cyber Appellate Tribunal mechanism for redressing the grievances of the aggrieved party against the orders of the Adjudicating officers

appointed under IT Act 2000 and 2008. There is one Cyber Appellate Tribunal (CAT) constituted under IT Act in the Country which is situated at New Delhi.

1.108On being asked about the existing number of Cyber Appellate Tribunals and their functioning, the Department, in their written reply, stated as under:-

> "There is one Cyber Appellate Tribunal established under IT Act in the Country. At present, the CAT is functioning at Jeevan Bharti (LIC) Building, New Delhi. The former Chairperson demitted the charge on 30.06.2011. Member (Judicial) joined on 20.12. 2011 and demitted the charge on 8.11.2012. During his tenure, Member (Judicial) organised meeting with the IT Secretaries of the respective State Governments and Police Officials dealing with the Cyber Crime Cases, reviewed the current status of disposal of cases in the States and identified the follow up action for expediting the disposal of cases. During the process of meeting, the stress was given on installation of Video Conferencing Equipment to facilitate the hearing of cases before the CAT by the litigants from the remote locations.
>
> Member (Technical) has taken over the charge in the month of December 2012. CAT is making efforts to discharge their responsibilities with the existing manpower and steps have been initiated to recruit additional manpower for its effective functioning. The efficacy of the Cyber Appellate Tribunal is being improved by creating necessary awareness in the public & the authorities and with efforts to deploy adequate manpower. The Act, however, provides for setting up Benches of CAT at different locations in the country.

1.109When the Committee desired to know the status of all the cases handled by CAT since its inception, the Department, in their written reply, stated as under:-

> "Since inception of Cyber Appellate Tribunal, 17 Appeals were disposed off by the former Chairperson. 21 Appeals are pending for hearing in the Tribunal which are scheduled for disposal on appointment of Chairperson. The Act, however, provides for setting up Benches in other parts of the country."

## II. Penalty

1.110The Department has furnished the details of existing penalty provision for different kinds of cyber-crime which is given at Annexure II.

1.111When the Committee desired to know the details of the incidences of cases registered and number of persons arrested for Cyber Crimes till date, the Department furnished the following data:-

| Sl. No. | Crime Head | Cases Registered | | | Persons Arrested | | |
|---|---|---|---|---|---|---|---|
| | | 2010 | 2011 | 2012 | 2010 | 2011 | 2012 |
| 1. | A. Offences under IT Act | | | | | | |
| 2. | Tampering computer source department | 64 | 94 | 161 | 79 | 66 | 104 |
| | Hacking Computer Systems | | | | | | |
| | i. Loss/damage to computer resource/utility | 346 | 826 | 1440 | 233 | 487 | 612 |
| | ii. Hacking | 164 | 157 | 435 | 61 | 65 | 137 |
| 3. | Obscene publication/transmission in electronic form | 328 | 496 | 589 | 361 | 443 | 497 |
| 4. | Failure | | | | | | |
| | i. Of compliance/orders of certifying authority | 2 | 6 | 6 | 5 | 4 | 4 |
| | ii. To assist to decoy or the information in interception by Govt. Agency | 0 | 3 | 3 | 0 | 0 | 3 |
| 5. | Un-authorised access/attempt to access of protected computer system | 3 | 5 | 3 | 6 | 15 | 1 |
| 6. | Obtaining Licence or Digital Signature by misrepresentation/suppression of fact | 9 | 6 | 6 | 4 | 0 | 5 |
| 7. | Publishing false digital signature certificate | 2 | 3 | 1 | 2 | 1 | 0 |
| 8. | Fraud Digital/Signature | 3 | 12 | 10 | 2 | 8 | 3 |
| 9. | Breach of confidentiality/privacy | 15 | 26 | 46 | 27 | 27 | 22 |
| 10. | Other | 30 | 157 | 176 | 17 | 68 | 134 |
| | **Total (A)** | **966** | **1791** | **2876** | **797** | **1184** | **1522** |
| | **B. Offences under IPC** | | | | | | |
| 1. | Public Servant Offences by/Against | 2 | 7 | 2 | 3 | 3 | 4 |
| 2. | False Electronic evidence | 3 | 1 | 4 | 4 | 1 | 2 |
| 3. | Destruction of electronic evidence | 1 | 9 | 9 | 0 | 10 | 16 |
| 4. | Forgery | 188 | 259 | 259 | 257 | 277 | 263 |
| 5. | Criminal Breach of Trust/Fraud | 146 | 118 | 282 | 100 | 129 | 215 |
| 6. | Counterfeiting | | | | | | |
| | i. Property/mark | 1 | 6 | 21 | 2 | 8 | 13 |
| | ii. Tampering | 8 | 5 | 19 | 12 | 7 | 26 |
| | iii. Currency/Stamps | 7 | 17 | 5 | 16 | 11 | 10 |
| | **Total (B)** | **356** | **422** | **601** | **394** | **446** | **549** |
| | **Grand Total (A+B)** | **1322** | **2213** | **3477** | **1191** | **1630** | **2071** |

1.112Keeping in view the growing instances of cyber-crime, the Committee desired to know as to whether the existing penalty is sufficient to act as deterrent for curbing cyber-crime. To this, the Department, in their written reply stated as under:-

> "As indicated ..x.x.x.. the IT Act 2000 addresses all aspects related to cyber crimes in a comprehensive manner with adequate deterrent provisions. In addition, the National Cyber Security Policy 2013 has provisions to enable development of a dynamic legal framework and its periodic review to address the cyber security challenges arising out of technological developments in cyber space."

## CHAPTER-VIII

## EDUCATION/AWARENESS/TRAINING

1.113When the Committee desired to know the details of the training/awareness programmes being conducted, the Department, in their written reply, stated that continuous efforts are being made to enhance the level of awareness of investigating agencies in the country. The following efforts have been made in this direction:

- Ministry of Home Affairs has issued an Advisory to the State Governments and Union Territory Administrations on Cyber Crime. State Governments have been advised to build adequate technical capacity in handling cyber crime including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of cyber crimes. Also, under the Cyber Crime Investigation programme, Ministry of Home Affairs is supporting the establishment of Cyber Crime Police Station (CCPS) and Cyber Crime Investigations and Forensic Training Facilities (CCIFTF) in each State / Union Territory of India under Police Modernization Scheme. Action also has been taken to set up a National Centre of Excellence exclusively devoted to render Cyber Forensic services and to act as National Research and Training Centre on Cyber Forensics.
- Government has formulated a set of investigation manuals with procedures for Search, Seizure Analysis and Presentation of digital evidence in courts. The manuals have been circulated to Law Enforcement Agencies in all States.
- A major programme has been initiated on development of cyber forensics tools, setting up of infrastructure for investigation and training of the users, particularly police and judicial officers in use of this tool to collect and analyse the digital evidence and present them in Courts.
- Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training to Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.
- Cyber forensics training lab has been set up at Training Academy of Central Bureau of Investigation (CBI) to impart basic and advanced training in Cyber Forensics and Investigation of Cyber Crimes to Police Officers associated with CBI. In addition, Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States.
- In collaboration with Data Security Council of India (DSCI), NASSCOM. Cyber Forensic Labs have been set up at Mumbai, Bangluru, Pune and Kolkata for awareness creation and training programmes on Cyber Crime investigation. National Law School, Bangalore and NALSAR University of

Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.

In XII plan also, capacity building and training mechanism for developing a strong and dynamic skilled work force for investigation of Cyber crimes has been identified as a focused area.

In addition, the recently approved National Cyber Security Policy-2013 provides for actions related to increasing the level of awareness and preparedness among investigating agencies in the country."

1.114When asked as to whether the Department has tried to measure the awareness level about tackling cyber threats in the officers/Government officials as well as in the common mass, the Department, in their written reply, stated as under:-

"In order to gauge the level of cyber security preparedness as well as awareness in the country, Department has initiated a project on 'National e-Security Index' in association with Data Security Council of India (DSCI). This project is expected to enable studies and surveys in different sectors and segments in the country and provide information in the form of an index that can guide policy related actions in the country."

1.115Further, with regard to the measures for creating awareness about cyber-crime in the country, when asked for the initiatives that have been taken by the Government to create awareness about cyber-crime since childhood, the Department provided the same reply which it had provided during the examination of Demands for Grants (2011-12), which is as under:-

"As part of the initiative on Internet security awareness, material in the form of presentations, posters, pamphlets, cartoons, guide books, security tools, parental controls etc. was designed for children. Awareness programmes are designed for parents, teachers & children and 150 workshops have been organized in schools across the country covering 20,000 students up to $10^{th}$ grade. Internet Security contests are organized for children and best posters are selected for making the yearly calendars. As part of this initiative, web portal titled 'www.infosecawareness.in' is also hosted."

## PART – II

## OBSERVATIONS/ RECOMMENDATIONS OF THE COMMITTEE

### Introductory

**Advent of internet has added a new dimension to the usage of computer in our day-to-day lives and exposed our lives to the complexities of cyber-crime. The Committee note that the 'anonymous' character and 'borderless' nature of the problem have made cyber security a major concern across the globe. It is being used to carry out multiple forms of cyber-crime *viz*. identity theft, financial fraud, stealing of corporate information, planting of malicious software (malware)/Trojans, conducting espionage, disrupting critical infrastructures, facilitating terrorist activities, etc. The emergence of mobile technology and cloud computing has further complicated the entire cyber security landscape. The Committee note from the website of C-DAC that as per the latest Report released by Internet Crime Complaint Centre of the United States, India ranks fifth among countries reporting maximum number of cyber crimes. The Committee also take cognizance of the key findings of the 'Internet Security Threat Report- 2013 (Volume 18)' of Symantec, USA wherein it has been stated that there was 42 per cent surge in global targeted attacks during 2012 as compared to 2011 and 30 per cent increase in web-based attacks. In addition, the Report also revealed that India has seen a 280 percent increase in BOT infections that are continuing to spread to larger number of emerging cities in India. The Committee are highly perturbed to note that 3,911 India's website were defaced/hacked upto June, 2013 and majority (around 2667 out of 3911) of these attacks occurred in the '.in' domain whose servers are in India. The Committee also note that while the usage of Internet has facilitated transparency and greater accountability, it has at the same time led to increasing forms of cyber crime and cyber threat each day with newer challenges for data protection and security. The Committee, while taking note**

**of the emerging threats in the cyber space which exceeds the level of preparedness because of being technology driven, took up the subject for detailed examination. The details of findings of the Committee associated with the subject are dealt with in the succeeding paragraphs.**

**Increase in Cyber-Crime Cases and Preparedness to tackle the issue**

**2.2 The Committee note that Indian cyber landscape has seen a significant increase in spam and phishing activities, virus and warm infections, Bot Net infected systems, etc. and were apprised of 20 types of cyber crime being witnessed worldwide. The Committee are sure by the time this Report is tabled many more computer viruses/malwares may have been reported/noticed making our systems more vulnerable and prone to attacks.**

**2.3 The Committee are concerned to note that the number of incidents of website compromise in India has grown 5.5 times during the last 5 years (2007-08 to 2013-14) making the country amongst top five countries with respect to spam mail. Further, the phishing incidents have increased from 392 to 887 during the same period. Resultantly cyber crime threat incidents handled by the Cert-In have also increased considerably during this period. Further, 20 different categories of threats have been identified against which whole cyber space is required to be protected. The Secretary, DeitY, during the course of evidence was candid in admitting that the nature and size of the threat in cyber space in India is looming large and it is very much important to protect eleven critical sectors such as power, atomic energy, space, aviation, transportation, etc. which are predominantly using IT systems. The Committee feel that in a rapidly changing scenario where all the systems are getting integrated rapidly through IT infrastructure and upcoming technologies such as cloud, it is imperative that our preparedness to face challenges emanating from any kind of cyber attack is hundred per cent full proof. Therefore, the**

**Committee recommend that the Department should put the proposed agenda of 24x7 National Critical Information Infrastructure protection centre, which aims to protect the critical information infrastructure in the country, on top priority and implement its cyber security programmes expeditiously so that any kind of cyber attack have no impact on functioning of our critical sectors.**

**(Para Nos. 2.2 and 2.3, Recommendation Sl. No. 1)**

**Cyber-Crime and financial loss**

**2.4 The Committee are concerned to note that there has been a consistent increase in cyber crime cases in the country during last five years. As per the cyber-crime data maintained by National Crime Records Bureau (NCRB), a total of 420, 966, 1791 and 2876 Cyber Crime cases were registered under Information Technology Act during the years 2009, 2010, 2011 and 2012 respectively, and a total of 276, 356, 422 and 601 cases were registered under Cyber Crime related Sections of Indian Penal Code (IPC) during 2009, 2010, 2011 and 2012 respectively. In addition, number of Cyber Crime cases registered by Central Bureau of Investigation (CBI) during the years 2010, 2011 and 2012 under provisions of Information Technology Act 2000 and other acts were 10, 12 and 11 respectively. The Committee find it disquieting to note that the quantum of financial loss and privacy related cases in the country due to cyber-attack/fraud in last few years have increased. According to the Reserve Bank of India (RBI), in the last five years though the number of fraud cases reported by Banks on account of ATM Debit Cards/Credit Cards/Internet have decreased from 15018 (in 2010) to 8322 (in 2012), yet the amount involved had increased from Rs. 40.48 crore in 2010 to Rs. 52.67 crore in 2012. Further, the number of cases registered by CBI pertaining to financial frauds under the provisions of Information Technology Act 2000 ranged between 6 to 8 during 2008 to 2011 and amount involved increased from Rs. 6.42 crore to Rs. 28.79 crore. The**

**Committee are of the view that the reported number of cases involving financial fraud due to cyber related cases is just tip of the iceberg as a number of cases go unnoticed and unreported.**

**2.5 The Committee are unhappy to note that as of now there are several agencies which are involved in maintaining separate data with regard to cyber crime cases. National Crime Records Bureau (NCRB) under Ministry of Home Affairs (MHA) is maintaining data on cyber frauds. The mechanism for recording data with regard to Internet financial frauds, along with quantum of loss, is being maintained by Reserve Bank of India and Central Bureau of Investigation (CBI). The Committee have been informed that DeitY regularly interacts with Banks, RBI and CBI regarding cyber frauds related actions such as prevention, investigation, support, technical advisories, promotion of best practices and compliances, yet in view of ever increasing incidence of cyber crime cases and their impact on country's security, finance and economy as a whole the Committee fail to understand as to how the Department concretises its cyber security strategies when so many agencies are involved in data collection and maintenance and when there is absence of any centralised monitoring system and centralised maintenance of data relating cyber fraud. The Committee feel that there should be one single, centralised cell/agency to deal with all cases of cyber crime/threat in the country. This will not only help the Department in knowing the pattern of the crime but also prevent recurrence of same kind of crimes with newer strategies. The Committee, therefore, recommend the Department to work in the above direction and apprise the Committee of the action taken in this regard.**

**(Para Nos. 2.4 and 2.5, Recommendation Sl. No. 2)**

**Challenges/ Constraints relating to human resource (Auditors, Cyber Security Experts and skill development in IT)**

**2.6 The Committee note that the complex inter-connectivity of Internet with borderless environment, evolving innovative technologies, lack of awareness and rapidly changing security and threat landscape has posed massive challenge to cyber security ranging from data theft, espionage and Denial of Service (DoS) attacks to offensive actions by adversarial State and Non-State actors. The Committee also note that anonymous attacks – groups sponsored by Nations and terrorist groups also have become a major cross border challenge in Cyber Space.**

**2.7 The Committee are unhappy to note that though all critical sector organizations under Central Government Ministries/Departments are mandated to implement information security best practices as per ISO 27001, there are 546 organizations in the country which have obtained the ISO 27001 certification. What is more intriguing is that the Department has not made any effort to ascertain as to why all the Government organisations have failed to obtain ISO 27001 certification. The Committee need not emphasise that adhering to information security best practices helps in containing the cyber crime to a great extent. Therefore, the Committee recommend the Department to take necessary steps in identifying the reasons for all the Government Departments/ organisations for not following the information security best practices and urge upon them to expeditiously obtain ISO 27001 certification to enable them to adhere to information security best practices.**

**(Para Nos. 2.6 and 2.7, Recommendation Sl. No. 3)**

**2.8 The Committee are given to understand that shortage of manpower is one of the major constraints in all the organisations involved in securing Indian cyber space. During the examination of Demands for Grants (2013-14), the Department had submitted that there is shortage of cyber security**

**experts/auditors/IT skill in the country. The Committee are extremely disturbed to note that even though challenges to cyber space are on the rise, in a country with a population of around 1.21 billion, so far only around 42,000 students have been trained/undergoing training in various long-term/short-term courses and along with the existing personnel, a total of about 65,000 trained personnel are available pertaining to cyber security as against the estimated requirement of 5 lakh trained personnel. Though the Department has taken initiatives such as conducting extensive training programmes as part of the Information Security, Education and Awareness Programme (ISEA) for increasing the number of cyber security experts in the Indian Government organisations and engaging the National Security Council Secretariat with the task of determining the extent of augmentation of Cyber Security experts in the Government organizations, the Committee feel these initiatives are far from adequate. This was echoed by the Secretary, DeitY, during the course of evidence when he said 'we still have a long way to go so far as manpower in IT is concerned'.**

**2.9 The Committee are also disappointed to note that there are only 97 Master trainers and 44 empanelled auditors by Cert-In in the country. The Department has submitted that the list of empanelled auditors has been brought down because they have to pass a stringent test. The Committee feel that while the quality and examination process cannot be compromised, the number of empanelled auditors is very less considering the requirement in the field and there is an urgent need to empanel more number of auditors to meet the requirement. The Department has also submitted that critical shortage of cyber security professionals need to be tackled in mission mode with innovative recruitment and placement procedures along with specialized training of existing manpower. The Committee, therefore, strongly recommend that the Department should make concerted efforts to increase the number of cyber**

**security experts/auditors/IT skill in the country on top priority basis so as to ensure that shortage of man power does not come in the way of securing Indian cyber space. The Committee may be kept apprised about the status of the increase of cyber security experts/auditors/IT skill in the country.**

**(Para Nos. 2.8 and 2.9, Recommendation Sl. No. 4)**

**Research and Development to secure Cyber Space**

**2.10 The Committee note that Research and development activities are being carried out by eminent universities/organisations in areas of cyber security which *inter-alia* include (a) Cryptography and cryptanalysis, (b) Network and System Security, (c) Monitoring and Forensics and (d) vulnerability remediation and the key priority of identified areas as identified by the Department is to carry out innovative R&D with focus on basic research, technology development and demonstration, setting up test-beds, transition, diffusion and commercialization leading to widespread deployment in the field to enhance security of cyber space in the country. The Committee are, however, concerned to note that funds allocation for R&D in cyber security during the year 2012-13 could not be utilized fully due to procedural compliance for settling of pending UCs and budget for the year 2013-14 has been cut down by Rs. 10 crore (approx). This budgetary cut is a matter of extreme concern particularly when the Department has stated that large funds need to be allocated to undertake development of key technologies and present funding provided to R&D in the area of Cyber Security does not allow undertaking projects for development of strategic technologies. The Committee feel that specialised research being an important and integral part of cyber security programme, adequate attention needs to be given to this aspect with sufficient funding. The Committee, therefore, recommend that the Department should immediately take necessary steps for optimum utilisation of funds under R&D in cyber security and also facilitate research in strategic technologies. The Department should also**

**facilitate in design of programmes for development/enhancement/promotion of skills/expertise for R&D in cyber security.**

**(Para No. 2.10, Recommendation Sl. No. 5)**

**Cyber Crime Cell and Cyber Crime Lab**

**2.11 The Committee note that there is Cyber Forensics training lab at Training Academy of Central Bureau of Investigation (CBI) to impart basic and advanced training in cyber forensics and investigation of cyber-crimes to Police Officers associated with CBI. The Committee also note that the Government has also set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States. The Committee are of the strong opinion that there is an urgent need to increase the number of cyber-crime cells and labs in the States and provide requisite manpower, training and infrastructure to them. The Committee, therefore, recommend the Department to take concrete initiatives in setting up the cyber-crime cells and labs in States where these do not exist and also upgrade and strengthen the existing cyber crime cells with adequate fund and infrastructure so as to cope up with the rapid cyber threat and privacy infringement.**

**(Para No. 2.11, Observation/Recommendation Sl. No. 6)**

**Budgetary allocations to tackle the Cyber threats**

**2.12 The Committee note that even though the expenditure pattern has been Rs. 20-30 crore on an average for each year for tackling cyber threat, a sum of Rs. 500 crore has been allocated for Twelfth Five Year Plan against the proposed sum of Rs. 1500 crore. The Secretary, DeitY, informed the Committee that the Department proposes to approach the Planning Commission for allocation of more funds. However, considering the quantum increase in allocation and**

**keeping in view the continuous under-utilisation of funds, the Committee trust that with higher allocations received for the current Plan period as compared to earlier years the Department will increase their capacity building for carrying the programmes so as to utilise the allocated funds and achieve the desired objectives.**

**(Para No. 2.12, Recommendation Sl. No. 7)**

**Threat from imported electronics/IT products and hosting of servers outside India (Need for Certification unit and hosting of servers in India)**

**2.13 The import of electronic/IT products and hosting of servers outside India pose major threat to the country's security in general and threat to the citizen's security and privacy in particular. The Committee in their Thirty-fourth Report on Demands for Grants (2012-13) had raised their concern over the risks involved with imported electronics/IT products and recommended the Department to take action in this regard. The Committee are, however, unhappy to note that the country depends largely on imported electronics and majority of the websites are still being hosted outside India. The Committee are given to understand that hosting of websites/servers outside India is largely on account of economical and cost advantage reasons because the protection mechanism for securing websites involves significant expenditure. The Department itself has admitted that there are Technical concerns *viz*. attack attribution for counter action and Legal concerns *viz*. cooperation and jurisdictional issues due to location of internet servers outside country. The Committee also note that the Government has adopted strategies to deal with the hassles which include issuance of advisories to all intermediaries including national and international service providers, regular dialogue with the intermediaries, notification of a 'Framework and Guidelines' for use of Social Media by its agencies, etc. In addition, the Department has drafted a 'e-mail policy' and 'data storage policy' for the Central Government and the State Governments which would not only mandate all Government employees to use**

**the Government mail services, but would also prohibit usage of private services hosted whether in India or abroad (as the confidential and nationally sensitive data etc. in 99 percent of the cases emanate from the Government organisations). While all these initiatives have been taken note of, keeping in view the security aspects the Committee emphasize that the Government should take measures, as far as possible, to locate internet servers for critical sectors within the country.**

**2.14 The Committee note that under the Common Criteria Project of DeitY, STQC has established the Indian Common Criteria Certification Scheme (IC3S) at STQC, New Delhi and a full-fledged laboratory at Kolkata, with a capability for testing and certification of security of IT Products as per International standards, ISO/IEC 15408, based on Common Criteria Standards up to EAL4. Presently, evaluations are undertaken for certification of IT products like operating systems of routers, switches and firewalls; security appliances upto EAL4. The Committee are happy to note that India has become 17$^{th}$ 'Authorizing Nation' under Common Criteria Recognition Arrangement (CCRA) and that henceforth the product tested and certified under Common Criteria Certification Scheme up to Assurance Level 4 (EAL4) are acceptable not only in India but also in other member countries of CCRA without re-testing under the mutual recognition arrangements. It is also noted that the present scope of certification is limited to network boundary protection device and general purpose operating systems and STQC does not have necessary expertise and knowledge in highly complex products such as Radar etc. The Committee have been informed that in view of increasing penetration of ICT in the country, STQC Directorate has initiated steps to enhance its capacity for testifying IT products as part of its action in Twelfth Plan. In addition, the sub group on testing and certification infrastructure under the Joint Working Group for public Private Partnership on Cyber Security also envisage setting up of such testing**

**Infrastructure with active participation from private sector. The Committee desire that all efforts should be made with due promptitude to create the infrastructure and to enhance the capacity of STQC for testing of IT products. The Committee also recommend the Department to host more and more servers in India. Not only this, the Department should also have stringent measures to safeguard the indigenous servers as most of the cyber attacks are in '.in' domain. In addition, the Department should lay down provisions for mandatory certification for all imported electronics/IT/telecom products and have certification centres in each State/UT specifically at all the airports/naval docks/ international borders.**

**(Para Nos. 2.13 and 2.14, Recommendation Sl. No. 8)**

**<u>Concerns associated with upcoming technology</u>**

**2.15 The Committee observe that National e-Governance Programme (NeGP) is one of the ambitious projects of the Government and the Department is planning to use 'Cloud computing' for e-Governance Programmes and for storing its data. The Committee also note that the Government of India has recently published GI Cloud (Meghraj) – 'Strategic Direction Paper' and 'Adoption and implementation Roadmap' as a part of this Cloud initiative which prescribes the precautions, standards and guidelines on security addressing the various challenges and risks and gives more clear dimension to the timelines of implementation. With regard to the usage of 'Cloud computing', the Committee in their Twenty-seventh Report (2011-12), had expressed apprehensions about technological and legal challenges associated with the concept of 'shared platform' and had recommended the Department to conduct a study/survey to find out the existing scenario nationally and internationally and be prepared with a mechanism to deal with the risks associated with the usage of Cloud computing and be vigilant about such emerging technologies. However, the Committee are surprised to note that though NeGP has entered seventh year of its implementation, the Department has neither conducted any study/survey in**

**this regard nor has any data on instances of cyber security breaches encountered in e-Governance projects. The Committee feel that NeGP being a visionary project of the Government, the Department should not show any laxity. The Committee, therefore, recommend the Department to conduct a study/survey to find out the instances of cyber security breaches in NeGP projects. While cautioning the Department to be extra vigilant with the usage of the new technology 'cloud' which is still at a nascent stage, the Committee desire that the Department would stick to their assurance of keeping security issues on priority, particularly, in the implementation of e-Governance projects and make the programme foolproof.**

**(Para No. 2.15, Recommendation Sl. No. 9)**

**<u>Co-operation/coordination with other organisations/countries (NCIIPC, all Ministries, Departments, Cyber Appellate Tribunal, CERT-In, Police) PPP and efficacy of organisations</u>**

**2.16 The Committee note that apart from Department of Electronics and Information Technology/Indian Computer Emergency Response Team (CERT-In) there are multiple organisations involved in securing India's cyber space *viz*. Ministry of Defence (MoD), Ministry of Home Affairs, Intelligence Bureau (IB), Department of Telecommunications, National Disaster Management Authority (NDMA), National Technical Research Organisation (NTRO), National Critical Information Infrastructure Protection Centre (NCIIPC), Research and Analysis Wing (RAW), etc. In addition, in order to address effectively the issue of overlapping responsibilities and enhancing coordination between the stakeholder agencies in the country, the Government has approved a framework and has tasked the National Security Council Secretariat (NSCS) to co-ordinate, oversee and ensure compliance of cyber security policies.**

**2.17 The Committee also note that one of the primary challenges facing both Government as well as Industry is to curb the cyber threat at the earliest and this cannot be achieved in isolation by either Government or Industry alone and**

**it requires joint efforts and collaboration. A Joint Working Group (JWG), set up under the chairpersonship of the Deputy National Security Advisor, to work out the details of the Roadmap for cyber security cooperation has inter-alia recommended for setting up of permanent mechanism for Public Private Partnership. While appreciating the initiatives and the coordination of Department of Electronics and Information Technology with various organisations, the Committee recommend the Department to implement the recommendations of the Working Group in a time bound manner.**

**(Para Nos. 2.16 and 2.17, Recommendation Sl. No. 10)**

**MoUs and International Treaties**

**2.18 The Committee note that in a globalised economy, a focused approach to international relations is vital particularly in case of cyber-space which by its very nature is borderless and anonymous. The Committee also note that the Department has taken numerous collaborative efforts and has geared up to encourage sustainable development and strengthening partnerships with other countries. In addition, 'National Cyber Security Policy (NCSP)-2013' provides for information sharing and cooperation arrangements with other countries to develop bilateral and multi-lateral relationships in the area of cyber security with other countries and to enhance national and global cooperation among security agencies, CERTs, Defence agencies and forces, Law Enforcement agencies and the judicial systems. The Committee are also given to understand that Department enters into international cyber security cooperation arrangements with organizations engaged in similar activities, in the form of Memorandum of Understandings (MoUs) and in case of absence of MoUs with some countries, the provisions of MLAT (Mutual Legal Assistance Treaty) are used for eliciting support for cyber crime cases. The Committee are happy to note that the Department has signed MoUs in the area of cyber security with USA, Japan, South Korea, Mauritius, Kazakhstan, and Finland and during the year 2012-13, MoU has also been signed with Canada in ICT and Electronics**

**sector. Further, the Department with active assistance of the Ministry of External Affairs, is also having engagement dialogue with several countries such as Malaysia, Israel, Egypt, Canada, Brazil that are willing to cooperate and share information with regard to cyber security incidents and vulnerabilities in IT products and systems. While appreciating the above initiatives, the Committee desire the Department to continue with these initiatives and enter into MOUs and exchange programmes with more number of countries for having legal and technical tie-ups for addressing the cross border challenges associated with cyber security.**

**(Para No. 2.18, Recommendation Sl. No. 11)**

**2.19 The Committee note that the Department has articulated on the need for global cyber jurisprudence in various international fora. The Committee also feel that in this era of inter-dependence and inter-connectivity, a separate discipline of cyber jurisprudence and new international court for cyber jurisprudence is the need of the hour which would go a long way in dealing with threats in cyber space. While admiring the initiatives taken by the Department, the Committee recommend the Department to redouble their efforts in making India a pioneering country for the cause of cyber jurisprudence.**

**(Para No. 2.19, Recommendation Sl. No. 12)**

**<u>Preparedness/Policies /legal Initiatives to address the issue (IT Act and Cyber Security)</u>**

**2.20 The Committee note that keeping in view the security risks and vulnerabilities of the internet/computer run systems like defence establishments, hospitals, transportation, Banks, Government organisations, Government has taken several steps to improve the alertness of the Government and other critical sector organisations and as part of Cyber Crisis Management Plan (CCMP) for countering cyber attacks and cyber terrorism , all Ministries/Departments of Centre/State Governments and their organisations and critical sectors have been mandated to continuously assess the posture of**

**their IT systems and networks. In addition, the Department has advised organizations to report the cyber security incidents to CERT-In within one hour of occurrence of the cyber attack incident or noticing the incident. The Committee recommend that CCMP should be frequently reviewed and revised so as to keep pace with the rapid changing nature of cyber threats. Further, DeitY should ensure that all the Central Ministries/Departments/ Organisations/State Governments implement the Cyber Crisis Management Plan (CCMP) in right earnest.**

**(Para No. 2.20, Recommendation Sl. No. 13)**

**2.21 The Committee have also been informed that there are provisions under Sections 43 A, 66 A, 67, 69 B, 70 (1), 70 (4), 70-B, 72 A, 79 and 84 A, in the Information Technology Act, 2000 (IT Act) to address to the problems relating to cyber crime. On the issue of adequacy of the existing legal frame work for dealing with the cyber-crimes, the Department has stated that IT Act, 2000 addresses all aspects related to cyber crimes in a comprehensive manner with adequate compliance and deterrent provisions and at present, there is no need to amend the Information Technology Act to address National Cyber Security Policy. At the same time, the Department has also stated that since it is a dynamic area, the IT Act will be amended as and when needed. The Committee are of the view that even though the existing provisions of IT Act, 2000 may seem adequate to address all aspects related to cyber crimes in a comprehensive manner in the present circumstances, in view of the recent uproars over Section 66A of IT Act and in the light of everyday development in the area, the Department needs to put in place a system of periodical review of the existing provisions in various Sections of the Act. The Committee, therefore, urge the Department to take the above issue seriously so as to have preparedness on all provisions as the entire country is rapidly becoming dependent on Information Technology.**

**(Para No. 2.21, Recommendation Sl. No. 14)**

**National Cyber Security Policy – 2013**

**2.22 The Committee note that in order to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country, the Department has prepared 'National Cyber Security Policy (NCSP) – 2013' in consultation with all relevant stakeholders, user entities and public. The aim of the policy is to facilitate creation of secured computing environment and enable adequate trust and confidence in electronic transactions and also guide stakeholders' actions for protection of cyber space. Out of 47 objectives outlined in NCSP-2013, 8 areas have been prioritized by the Department. However, the Committee find it strange to note that NCSP does not depict any deadline/target except for the skilled force and it lacks detailed picture/road map for achieving all the goals of National Cyber Security Policy. On the issue of tentative deadlines by which the rules/guidelines for NCSP-2013 would be in place, the Committee are given to understand that DeitY has already initiated steps to identify the follow up actions as well as agencies responsible and timelines for such actions. The Government is in the process of preparing individual schemes which are to be implemented by the Government and the Joint Working Group set up under the aegis of National Security Council Secretariat (NSCS). Further, the Department has assured to implement major programmes in the next one year. While appreciating the aims and objectives of the NCSP which is definitely a step forward, the Committee urge the Department to chalk out the definite targets/time frame on priority areas with fixing up of responsibilities of different agencies involved/to be involved. The Department should ensure that the micro plans of the Policy are worked out at the earliest and implementation takes off during 2014 itself so as to address the urgent need of dealing with the cyber security threats and the need to build capacity in the country in terms of**

**infrastructure, preventive and protective legal actions, grievance redressal mechanism, evaluation and compliance verification for imported IT product, certification, awareness, etc. The Department must also ensure that the NCSP-2013 policy which is expected to facilitate creation of secured computing environment and enable adequate trust and confidence for the IT users in the country meets its objectives.**

**(Para No. 2.22, Recommendation Sl. No. 15)**

**<u>Cyber Security and Right to Privacy</u>**

**2.23 The Committee note that balancing cyber security and right to privacy is extremely complex. The Committee are given to understand that in the absence of any Bill on privacy, the Information Technology Act 2000 as amended in 2008 takes care of data privacy and data protection. The Act contains adequate provisions to deal with various cyber related offenses as well as protection of privacy of individuals. These provisions include Section 43 and section 66 for penalty and stringent punishment for hacking of website, Section 43A - for compensation to the affected person for failure to protect data, Section 72-for penalty for breach of confidentiality and privacy, Section 72A-for punishment for disclosure of information in breach of lawful contract. In addition, The Information Technology Rules (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information), 2011 notified on 11th April, 2013 under section 43A of the Information Technology Act defines the sensitive personal data and reasonable security practices and procedures. The Rules require body corporate to provide policy for privacy and disclosure of information (Rule 4), obtain consent of user for collection of information (Rule 5), prior permission required from provider of information before disclosure of sensitive personal information (Rule 6). While the above provisions have been taken note of, the Committee are extremely unhappy to note that the Government is yet to institute a legal framework on privacy. When asked about**

**the status of the above legislation, the Department has diverted the issue stating that the Department of Personnel and Training is still in the process of evolving legislation to address concerns of privacy, in general, and it is still at the drafting stage. The Committee seriously feel that in view of enormous data, very sensitive in nature, being consigned to cyber space each day particularly in the light of Government's visionary UIDAI programme, the Government should not jeopardize the privacy of citizens on the plea that the Department is concerned only with Section 43(A) which it is based on self-regulation. Though the Department has stated that personal information may not come under the purview of DeitY, the Committee are of the opinion that the Department should carry out their responsibilities at least with regard to the digital data. The Committee, while acknowledging the complex nature of the cyber space and the maturity and competence required in balancing cyber security and right to privacy, desire that the Department in coordination with the Department of Personnel and Training, multi-disciplinary professionals/experts should come out with a comprehensive and people friendly policy which may protect the privacy of citizen and is also foolproof from security point of view.**

**(Para No. 2.23, Recommendation Sl. No. 16)**

**2.24 While taking note of the Department's stand on the recent instances of surveillance and interception of data (though only meta-data) by other countries, that incursion into the content of the country's data will not be tolerated, the Committee are of the strong opinion that the Department should have exercised enough caution so that such a situation was not allowed to occur at the first instance. Further, the Committee feel that the Department should be extremely vigilant and cautious in terms of safety as well as in terms of policy with different countries so as to avoid such leakage and interception of sensitive data in the name of surveillance. The Committee, therefore, strongly recommend the Department to take remedial measures and come out with a**

**policy which should be implemented stringently so as to obviate recurrence of such instances.**

**(Para No. 2.24, Recommendation Sl. No. 17)**

**Grievance redressal mechanism**

**2.25 The Committee note that the existing system for registering complaints for grievance redressal regarding cyber-crime involves reporting with the local police stations or cyber-crime cells of law enforcement agencies, however, further redressal process of such cases is similar to other crime related cases. The Committee are given to understand that since Law and Order is a State subject, all actions related to crime including cyber crime are dealt with by respective States/UTs and relevant data of such cases are being maintained by National Crime Records Bureau (NCRB). Further, many of the States have set up cyber crime cell which are monitoring such crimes. In view of the fact that there is steep rise in cyber-crime instances and the rate at which common man in our country is affected, the Committee are surprised to learn that not all the States have a separate cyber crime cell and there is no centralized system/cell for monitoring cyber-crime. The Committee, therefore, recommend the Department for having mandatory cyber-crime cell not only in each state but also in each District and Block. The Committee also recommend for having a centralized system/cell for monitoring cyber-crime which would have real-time details of registration and disposal status of cyber-crime throughout the country. The Department may also expedite follow up with the Ministry of Home Affairs about the Department's request to increase the awareness among people regarding the mechanism of reporting cyber crime cases with the cyber crime cells of law enforcement agencies.**

**(Para No. 2.25, Recommendation Sl. No. 18)**

**Cyber Appellate Tribunal (earlier known as Cyber Regulations Appellate Tribunal)**

**2.26 The Committee note that the Cyber Regulations Appellate Tribunal (CRAT) was established in October, 2006 in accordance with the provision contained under Section 48(1) of the IT Act 2000, and after the amendment of the IT Act in the year 2009, the Tribunal is known as Cyber Appellate Tribunal (CAT). As per the IT Act, any person aggrieved by an order made by the Controller of Certifying Authorities or by an Adjudicating Officer under the Act can appeal before the Cyber Appellate Tribunal (CAT). The main objectives of the Cyber Appellate Tribunal is to consider and decide the validity/legal propriety of the orders passed by the Adjudicating Officers and to spread awareness about the Cyber Appellate Tribunal (CAT) mechanism for redressing the grievances of the aggrieved party against the orders of the Adjudicating officers appointed under IT Act 2000 and 2008. The Committee also note that till date there is only one Cyber Appellate Tribunal in the country though the Act provides for setting up Benches in other parts of the country which has not yet been done. The Committee are surprised to learn that since inception of CAT only 17 appeals have been disposed off by the former Chairperson and 21 appeals are still pending for hearing in the Tribunal which are scheduled for disposal on appointment of the new Chairperson. The Committee are also given to understand that Member (Technical) has taken over the charge in the month of December 2012 and CAT is making efforts to discharge their responsibilities with the existing manpower and steps have been initiated to recruit additional manpower for its effective functioning. While expressing their displeasure over the undue delay taking place in disposal of appeal by the Cyber Appellate Tribunal, the Committee strongly recommend the Department to deploy adequate manpower at the earliest so that appeals that are pending for hearing in the Tribunal are disposed of expeditiously. Efforts may also be made to set up CAT branches in other parts of the country, if need arises. The Committee may be kept apprised about the disposal status of cases before CAT.**

**(Para No. 2.26, Recommendation Sl. No. 19)**

**Education/Awareness/Training**

**2.27 The Committee appreciate that the Ministry of Home Affairs has advised State Governments and Union Territory Administrations to build adequate technical capacity in handling cyber crime including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of cyber crimes. The Committee also note that the Government has formulated a set of investigation manuals with procedures for Search, Seizure Analysis and Presentation of digital evidence in courts. The manuals have been circulated to Law Enforcement Agencies in all States. In view of technical expertise required in handling cyber crime, the Committee are of the opinion that mere issuance of advisories would not solve the problem. Rather, the Department should proactively coordinate with the Ministry of Home Affairs/State Governments for building up the capacity/training police personnel for detection, registration, investigation, handling of cyber crime evidences, etc.**

**(Para No. 2.27, Recommendation Sl. No. 20)**

**2.28 The Committee further note that in order to gauge the level of cyber security preparedness as well as awareness in the country, the Department has initiated a project 'National e-Security Index' in association with Data Security Council of India (DSCI) and the project is expected to enable studies and surveys in different sectors and segments in the country and provide information in the form of an index that can guide policy related actions in the country. The Committee recommend that the project should be implemented expeditiously and the Committee may be apprised of its status/outcome.**

**(Para No. 2.28, Recommendation Sl. No. 21)**

**2.29 The Committee are extremely unhappy to note that when asked about the initiatives taken by the Government to create awareness about cyber-crime**

**amongst children, the Department has furnished exactly the same reply that was provided to the Committee during the examination of Demands for Grants (2011-12) which *inter-alia* include 150 workshops organised in schools covering 20,000 students upto 10th Grade. In view of the non-availability of updated information, the Committee are unable to assess the action taken by the Department after 2011 and are not sure whether awareness/workshops have been conducted by the Department thereafter. The Committee would like the Government to take up projects/schemes for awareness programmes for children on continuous basis. The Department should also take necessary action in coordination with concerned authorities to make the curriculum of cyber security mandatory in schools syllabus. In addition to this, the Committee also recommend the Department to set up a national help line/call centre for common public which can guide them about dealing with cyber crime and redressal mechanism. The Committee may be apprised about the Department's concrete action in this regard.**

**(Para No. 2.29, Recommendation Sl. No. 22)**

**RAO INDERJIT SINGH**
**Chairman,**
**Standing Committee on**
**Information Technology**

**New Delhi**
**10 February, 2014**
**21 Magha, 1935 (Saka)**

**Annexure I**

*Vide Para 1.6 of the Report*

**List of top 20 countries with highest number of internet users**

| Sl. No. | Country or region | Population, 2011 Estimate | Internet Users latest data | % Population (Penetration) | Growth 2000-2011 | % of World Users |
|---|---|---|---|---|---|---|
| **1.** | China | 1,33,67,18,015 | 48,50,00,000 | 36.30% | 2055.56% | 23.00% |
| **2.** | United States | 31,32,32,044 | 24,50,00,000 | 78.20% | 156.94% | 11.60% |
| **3.** | India | 1,18,91,72,906 | 10,00,00,000 | 8.40% | 1900.00% | 4.70% |
| **4.** | Japan | 12,64,75,664 | 9,91,82,000 | 78.40% | 110.67% | 4.70% |
| **5.** | Brazil | 20,34,29,773 | 7,59,82,000 | 37.40% | 1419.64% | 3.60% |
| **6.** | Germany | 8,14,71,834 | 6,51,25,000 | 79.90% | 171.35% | 3.10% |
| **7.** | Russia | 13,87,39,892 | 5,97,00,000 | 43.00% | 1825.81% | 2.80% |
| **8.** | United Kingdom | 6,92,98,362 | 5,14,42,100 | 82.00% | 234.04% | 2.40% |
| **9.** | France | 6,51,02,719 | 4,52,62,000 | 69.50% | 432.49% | 2.10% |
| **10.** | Nigeria | 15,52,15,573 | 4,39,82,200 | 28.30% | 21891.10% | 2.10% |
| **11.** | Indonesia | 24,56,13,043 | 3,96,00,000 | 16.10% | 1880.00% | 1.90% |
| **12.** | Korea | 4,87,54,657 | 3,94,40,000 | 80.90% | 107.14% | 1.90% |
| **13.** | Iran | 7,78,91,220 | 3,65,00,000 | 46.90% | 14500.00% | 1.70% |
| **14.** | Turkey | 7,87,85,548 | 3,50,00,000 | 44.40% | 1650.00% | 1.70% |
| **15.** | Mexico | 11,37,24,226 | 3,49,00,000 | 30.70% | 1186.68% | 1.70% |
| **16.** | Italy | 6,10,16,804 | 3,00,26,400 | 49.20% | 127.47% | 1.40% |
| **17.** | Phillippines | 10,18,33,938 | 2,97,00,000 | 29.20% | 1385.00% | 1.40% |
| **18.** | Spain | 4,67,54,784 | 2,90,93,984 | 62.20% | 440.00% | 1.40% |
| **19.** | Vietnam | 9,05,49,390 | 2,92,68,606 | 32.30% | 14534.30% | 1.40% |
| **20.** | Argentina | 4,17,69,726 | 2,75,68,000 | 66.00% | 1002.72% | 1.30% |
| | | | | | | |
| **Top 20 countries** | | 4,57,89,50,118 | 1,60,17,72,290 | 35.00% | 481.57% | 75.90% |
| **Rest of the World** | | 2,35,11,05,036 | 50,89,93,520 | 21.60% | 494.89% | 24.10% |
| **Total World-Users** | | 6,93,00,55,154 | 2,11,07,65,810 | 30.50% | 484.72% | 100.00% |

**Annexure II**

*Vide Para 1.110 of the Report*

## Existing penal provisions for different cyber crimes under IT Act 2000

| Cyber Attacks/Crime | Brief Description | Sections Relevant in IT Act, 2000 and Amendments |
|---|---|---|
| Cyber Stalking | Stealthily following a person, tracking his internet chats. | 43, 66 (Compensation and punishment of three years with fine) |
| Intellectual Property Crime | Source Code Tampering etc. | 43, 65, 66 (Compensation and punishment of three years with fine) |
| Salami Attack (Theft of data or manipulating banking account) | Deducting small amounts from an account without coming in to notice, to make big amount | 43, 66 (Compensation and punishment of three years) |
| E-Mail Bombing | Flooding an E-mail box with innumerable number of E-mails, to disable to notice important message at times. | 43, 66 (Compensation and punishment of three years) |
| Phishing | Bank Financial Frauds in Electronic Banking | 43, 66, 66C (Compensation and punishment of three years with fine) |
| Personal Data Theft | Stealing personal data | 43, 43A, 72A (Compensation and punishment of three years with fine) |
| Identity Theft | Stealing Cyberspace identity information of individual | 43 (Compensation and punishment of three years with fine) |
| Spoofing | Stealing Credentials using, friendly and familiar GUI's | 43, 66 (Compensation and punishment of three years with fine) |
| Data Theft | Stealing Data | Provisions under 43, 43A, 65,66 and 72 (Compensation and punishment of three years with fine) |
| Worms Trojan Horses, Virus etc. | Different Hacking mechanisms | 43, 66 (Compensation and punishment of three years with fine) |
| Sabotage of Computer | Taking control of computer with the help of malware. | 43, 66 (Compensation and punishment of three years with fine) |
| DOS, DDOS Demat of Service | Flooding a computer with Denial of Service Attacks, DDOS is Distributed DOS attack | 43, 66, 66F (Compensation (up to life imprisonment under 66F) |
| Web Defacing | Web Pages Defacing | 43, 66 (Compensation and punishment of three years with fine) |
| Logic Bomb | Attack triggers on an event | 43, 66 (Compensation and punishment of three years with fine) |
| ATM fraud/EDI | Financial fraud in ATM and e- | 43, 66 |

| | | |
|---|---|---|
| | Commerce EDI | (Compensation and punishment of three years with fine) |
| Data Diddling | Modifying data for the process and retaining data integrity in the structures | 43, 65, 66<br>(Compensation and punishment of three years with fine) |
| Money Laundering on Web | Temporarily keeping a Web service for collecting money illegally, without registering with the any regulating authority for avoiding tax. | 43, 66, 66C, 66D and 72<br>(Compensation and punishment of three years with fine) |
| Spam and spoofing | Unsolicited E-mails | 43, 66A, 66D<br>(Compensation and punishment of three years with fine) |
| Publishing or transmitting obscene material | Publishing Obscene in Electronic Form | 67<br>(Punishment of three years with fine) |
| Pornography | Publishing or transmitting material containing sexually explicit act | 67A<br>(Punishment of five years with fine) |
| Child Pornography | Publishing Obscene in Electronic Form involving children | 67B |
| Video Voyeurism and violation of privacy | Transmitting Private/Personal Video's on internet and mobiles | 66E<br>(Punishment of three years with fine) |
| Phishing and Identity Theft | Sending Phishing mail, spoofing | 66D<br>(Punishment of three years with fine) |
| Dishonestly receiving stolen computer/ communication device | Stolen System | 66B<br>(Punishment of three years with fine) |
| Cyber Terrorism | | 66F<br>(Up to life imprisonment) |
| Offensive messages | Communication of offensive messages through computer/phone | 66A<br>(Punishment of three years with fine) |
| Refusal to facilitate and cooperate in Lawful interception | Refusal Lawful interception and refusal to cooperate in decrypting message | 69, 69A, 69B<br>(Punishment of seven years with fine) |
| Hacking of Protected Systems | Protection of Information Infrastructure | 70<br>(Punishment of ten years with fine) |
| Tampering with computer source programme | | 43, 65<br>(Compensation and punishment of three years with fine) |
| Intentionally or knowingly non compliance with the provisions of IT Act, rules or regulations made there under | | 68<br>(Punishment of two years) |
| Cheating using digital signature of other person | | 66C<br>(Punishment of three years with fine) |

**Appendix-I**

**STANDING COMMITTEE ON INFORMATION TECHNOLOGY**
**(2012-13)**

**MINUTES OF THE FOURTEENTH SITTING OF THE COMMITTEE**

---

The Committee sat on Tuesday, the 9th July, 2013 from 1100 hours to 1245 hours in Committee Room 'G-074', Parliament Library Building, New Delhi.

**PRESENT**

**Shri Rao Inderjit Singh–Chairman**

**MEMBERS**

***Lok Sabha***

2. Shri Abdul Rahman
3. Shri Rajendra Agrawal
4. Shri Nikhil Kumar Choudhary
5. Shri A. Ganeshamurthi
6. Smt. Darshana Jardosh
7. Shri Baidya Nath Prasad Mahato
8. Dr. Thokchom Meinya
9. Shri Tapas Paul

***Rajya Sabha***

10. Shri Joy Abraham
11. Shri Mohammed Adeeb
12. Shri Salim Ansari
13. Shri Bharatsinh Prabhatsinh Parmar
14. Dr. C.P. Thakur

***SECRETARIAT***

| | | | |
|---|---|---|---|
| 1. | Shri Brahm Dutt | - | Joint Secretary |
| 2. | Shri N.C. Gupta | - | Director |
| 3. | Shri A.K. Garg | - | Additional Director |
| 4. | Dr. Sagarika Dash | - | Deputy Secretary |

**Representatives of the Department of Electronics and Information Technology**

| | | |
|---|---|---|
| 1. | Shri J. Satyanarayana | Secretary |
| 2. | Dr. Gulshan Rai | Director General, CERT-In |
| 3. | Shri Rajendra Kumar | Joint Secretary |

2. At the outset, the Chairman welcomed the Members to the sitting of the Committee convened for having a briefing by the representatives of the Department of Electronics and Information Technology in connection with examination of the subject 'Cyber Crime, Cyber Security and Right to Privacy'.

[The representatives of the Department were then called in]

3. The Chairman welcomed the representatives of the Department of Electronics and Information Technology to the sitting of the Committee and drew their attention to Direction 55(1) of the Directions by the Speaker, Lok Sabha regarding confidentiality of the proceedings and Direction 58 regarding evidence liable to be treated as public.

4. After introductions by the witnesses, with the permission of the Chairman, the Secretary of the Department provided an overview of the cyber crime and cyber security of the country and then the Director General, CERT-In made a Powerpoint presentation covering various aspects of the subject *viz*. overall scenario of internet infrastructure, cyber crime and cyber security, malicious activities in international cyber space, types and trends in cyber security breaches, incidents being handled by the Department, issues and challenges in securing cyber space, National Cyber Security Policy, steps to secure the cyber space, balancing privacy and cyber security, etc.

5. The Committee, thereafter, sought clarifications regarding India's preparedness to tackle increasing cyber threats, International scenario and Memorandum of Understanding with other countries, implementation of the National Cyber Security Policy – 2013, sufficiency of budgetary provision, amendments proposed in Information Technology Act, 2000 etc. These were replied to by the witnesses.

[The witnesses then withdrew]

*A copy of verbatim proceedings of the sitting has been kept on record separately.*

**The Committee, then, adjourned.**

**Appendix-II**

## STANDING COMMITTEE ON INFORMATION TECHNOLOGY (2012-13)

## MINUTES OF THE SEVENTEENTH SITTING OF THE COMMITTEE

---

The Committee sat on Friday, the 23rd August, 2013 from 1500 hours to 1640 hours in Committee Room 'D', Parliament House Annexe, New Delhi.

**PRESENT**

**Shri Rajendra Agarwal – In the Chair**

**MEMBERS**

***Lok Sabha***

2. Shri Abdul Rahman
3. Shri Nikhil Kumar Choudhary
4. Shri Khagen Das
5. Shri Baidya Nath Prasad Mahato
6. Dr. Prasanna Kumar Patasani

***Rajya Sabha***

7. Shri Joy Abraham
8. Shri Mohammed Adeeb
9. Shri Salim Ansari
10. Dr. C.P. Thakur

***Secretariat***

| | | | |
|---|---|---|---|
| 1. | Shri Brahm Dutt | - | Joint Secretary |
| 2. | Shri Ajay Kumar Garg | - | Additional Director |
| 3. | Dr. Sagarika Dash | - | Deputy Secretary |

**List of representatives of the Department of Electronics and Information Technology**

| | | |
|---|---|---|
| 1. | Shri J. Satyanarayana | Secretary |
| 2. | Dr. Gulshan Rai | Director General, CERT-In |
| 3. | Dr. Rajendra Kumar | Joint Secretary |
| 4. | Shri S.S. Sarma | Additional Director |

2. At the outset, in the absence of the Chairman, the Committee chose Shri Rajendra Agarwal, a Member of the Committee, to act as the Chairman for the sitting in accordance with Rule 258(3) of the Rules of Procedure and Conduct of Business in Lok Sabha.

3. The Chairman welcomed the Members to the sitting of the Committee convened to take evidence of the representatives of the Department of Electronics and Information Technology in connection with examination of the subject 'Cyber Crime, Cyber Security and Right to Privacy'.

**(The representatives of the Department were then called in)**

4. The Chairman, then, welcomed the representatives of the Department of Electronics and Information Technology to the sitting and drew their attention to the provisions of Direction 55(1) of the Directions by the Speaker, Lok Sabha regarding confidentiality of the proceedings till the Report on the Bill is presented to the House and Direction 58 regarding evidence liable to be treated as public.

5. After introductions by the witnesses, with the permission of the Chairman, the Secretary of the Department provided an overview of the subject and thereafter elaborated on several aspects pertaining to Cyber crime and cyber security which are as follows:-

i. Threat posed by cyber attacks;
ii. New initiatives with regard to e-mail usage by the Government of India, acceptable Internet usage policy;
iii. Strategic paper called - 'Meghraj', on Cloud usage by Government;
iv. Security certification/testing of electronic/telecom equipment;
v. Adequacy of human resource, Infrastructure, R&D and fund for cyber security; and
vi. Readiness/crisis Management Plan and strategy to implement National Cyber Security Policy.

5. The Committee, thereafter, sought clarifications on various issues *viz*. types of cyber crime covered under IT Act particularly 'Phishing', financial losses occurring due to cyber attacks, existing mechanism of handling cyber crimes, penal provision and its adequacy, mode of protecting individual/commercial/Government information and issues associated with Right to Privacy, empanelment of auditors, Public Private Partnership, issues associated with connectivity of internet and cross border cyber attacks like international cooperation, hosting of servers, etc. They were replied to by the witnesses. The Committee also directed the representatives of the Department to furnish documents/copies of various policies released by the Department which were not readily available with them.

**(The witnesses then withdrew)**

A copy of verbatim proceedings of the sitting has been kept on record separately.

**The Committee then adjourned.**

**Appendix-III**

## STANDING COMMITTEE ON INFORMATION TECHNOLOGY (2013-14)

## MINUTES OF THE SEVENTH SITTING OF THE COMMITTEE

---

The Committee sat on Monday, the 10th February, 2014 from 1000 hours to 1030 hours in the Chamber of Hon'ble Chairman, Room No. 145-A, Third Floor, Parliament House, New Delhi.

### PRESENT

**Shri Rao Inderjit Singh–Chairman**

### MEMBERS

***Lok Sabha***

2. Shri Rajendra Agrawal
3. Shri Khagen Das
4. Dr. (Prof.) Thokchom Meinya
5. Dr. (Prof.) Prasanna Kumar Patasani
6. Shri Radhe Mohan Singh (Gazipur)
7. Smt. Seema Upadhyay

***Rajya Sabha***

8. Shri Salim Ansari
9. Shri Basawaraj Patil
10. Dr. Kanwar Deep Singh

***SECRETARIAT***

| | | | |
|---|---|---|---|
| 1. | Shri Brahm Dut t | - | Joint Secretary |
| 2. | Shri N.C. Gupta | - | Director |
| 3. | Shri A.K. Garg | - | Additional Director |
| 4. | Dr. Sagarika Dash | - | Deputy Secretary |

2. At the outset, the Chairman welcomed the Members to the sitting of the Committee convened to consider two original Reports viz. (i) Draft Report on 'Cyber Crime, Cyber Security and Right to Privacy' relating to Department of Electronics and Information Technology (Ministry of Communications and Information Technology) and (ii) ..xx..xx... The Committee, then, took up for consideration the Reports and adopted the same without any modification. The Committee, then, authorized the Chairman to finalize and present the Reports to the House.

3. The Committee placed on record their appreciation for the assistance rendered to them by the officials of Lok Sabha Secretariat attached to the Committee.

**The Committee, then, adjourned.**

xxxxxxx