Chapter 6
Role of Government in Tackling Cyber Security Threat

Pinosh Kumar Hajoary and K. B. Akhilesh

Abstract Cyber security was seen a technical problem, but humans are players in every Cyber security attack-defense game. This paper aims to provide a comprehensive critical assessment of role of government in tackling and implementing cyber security policy in India. While the role of the government is to provide safe and secure cyberspace in the country to its citizens. However, this paper highlights the current policies and recommends future Cyber security policy for creating a robust framework for protecting the Indian Cyber Space from attackers. It also explains the current trends of cybercrime, types of crime in India and provides direction for future collaborative framework for Cyber security prevention.

Keywords Cyber security · Digital India · Role of Government · Cyber security prevention framework · Cyber security policy · CERT-In · NCRB

6.1 Introduction

Cyber security is a defensive technique of protecting integrity of computers, networks, data, programs from the unauthorized access or damage or attack that are solely for misuse. It is commonly referred to as a set of activities both technical and non-technical undertaken to protect computers, networks and hardware and software devices. Cyberspace is a virtual network of networks that is used to store, modify and communicate information. It is a platform where an interaction between people, software and system takes place along with the World Wide Web. Cyber security was seen a technical problem, but humans are players in every cyber security attack-defense game. Cyber security consists of four important areas, i.e., application secu-

P. K. Hajoary (✉) · K. B. Akhilesh
Department of Management Studies, Indian Institute of Science, Bengaluru, India
e-mail: pinoshh@iisc.ac.in

K. B. Akhilesh
e-mail: kba@iisc.ac.in

K. B. Akhilesh and D. P. F. Möller (eds.), *Smart Technologies*,
https://doi.org/10.1007/978-981-13-7139-4_6

rity, information security, disaster recovery and network security. Cities are getting smarter, communities across the globe are rapidly turning to smart modern devices and applications to connect to various facilities like transportation, health, financial services and retail. Government of India is pushing hard for e-governance, digital connectivity in the country by providing affordable services to the common people. The core part of Government of India policy is concentrated on empowering society with flagship program called as "Digital India". However, success of this program is possible only when the data of the people are secured properly by implementing strict norms and robust monitoring system. Rapid up gradation of technology along with the evaluation of Internet of Things, there are more than 25 billion connected devices according to CISCO (2011). The figure will go up to 50 billion by 2020. Indeed, such devices are vulnerable to various forms of cyber-attack. In fact, as per HP survey report 70% devices are vulnerable to such attacks. India has the population of 1.32 billion as per 2016 survey and is the second largest population in the world. As per Government of India report, 50% of Indian population is under the age of 25 whereas more than 65% under the age of 35. By the year 2020, Indian's youth population average age would be 29 years. Currently, India has more than 450 million Internet users and is expected to reach 500 million by the year end (IAMAI, 2018). According to RBI midterm financial inclusion report for 2015, more than 50% of Indian youths participated in the financial system. As e-commerce continues to grow at 30% (December 2011–2015), the Indian digital commerce market stands at Rs. 1, 25,732 crores. Hence digital divide will slowly narrow down with various initiatives undertaken by the government. Securing data, cyber-rumor and fake news have become a major concern for the government to handle. For example, Aadhaar data security has become a major concern for the citizens of the country because of data breach in the system. Aadhaar card is twelve-digit unique identity number issued by Unique Identification Authority of India (UIDAI) to all its citizens based on their demographic and biometric data. It is the world's biggest and most successful biometric ID system with around 1.19 billion formulated in the system. Data safety and protection have been a sensitive issue for the people in India. Not much have been done regarding data safety and security by the government. Cyber-physical system covers extremely wide range of applications. Examples of new generation of systems that rely on cyber-physical technology such as advanced automotive systems, assisted living, smart homes, avionics, critical infrastructure control like electric power and communication systems, defense systems, distributed robotics, energy conservation, environmental control, manufacturing, medical devices and systems, process control, smart structures, traffic control and safety. Gemalto, a digital security firm, has claimed that 3.24 million records were compromised in India in the year 2017 which has exponentially increase whopping 783% from the previous years.

6.1.1 Introduction to Sector

Digital India in a digital world has witnessed a rapid rise in Internet access and information sharing which is generally termed as "Information age." It is alleged that the total volume of digital data storage will be around 44 zettabytes (44 trillion gigabytes) by the year 2020 as per IDC, EMC Digital Universe with research and analysis finding team (IDC, 2014). Much of those data will consist of personal information including the data of the product purchased, places traveled, and those data created from smart, intelligent connected devices in the Internet. Government of India launched a flagship program called "Digital India" on July 1, 2015 to ensure seamless government services to the citizens and improve digital infrastructure in the country. This initiative involves integration of digitization of governance, health care and educational services, cashless transaction, transparency in bureaucracy, equal distribution of welfare schemes to empower common citizens of India. However, one of the visions of Government of India is to provide safe and secure cyberspace in the country (PIB, 2014). Such initiative and vision will be successful only when government plays an active role in providing citizens with robust full proof cyber security policies and play an active role in building secure cyberspace. Cyber security of the country is a paramount important for the government and its people for the safety and security. Most of the public services in India are wholly controlled by the government-led system. Hence such system needs a robust and full proof security for smooth functioning. Reserve bank of India and Insurance Regulatory Development Authority of India (IRDA) have time and again released various guidelines to its citizens. However, these guidelines are failing short of preventing sophisticated attacks in the current scenario. The common people in India are unaware of the various cyber-frauds, scams and cyber-attacks taking place in the country. The role of the government is to develop sophisticated security layers, IT policies, Cyber security policies and set up benchmark for best practices in the country. Recently, India and Singapore have signed Memorandum of Understandings (MoU) in the areas of Cyber security to share information, expertise in fighting cybercrime in both the countries.

6.1.2 Cyber Security Landscape

Over the years, Cyber threat has evolved themselves and transformed with changing environment. The regulatory landscape in India is compelled to change slowly with each passing day with increasing cyber-attacks in recent years. A brief picture of transformation of Cyber security is depicted in Table 6.1.

Table 6.1 Transformation of cyber security

Mainframes	Client/server	Internet	E-commerce	Digital
1970s	1980s	1990s	2000	Recent times
Natural hazards Physical response measures in place. Like evacuation and first aid	Dependence on few new technologies Elementary disaster response to system failures Virus protection developed	Enterprise-wide risk management introduced Common regulatory compliance policy Business continuity focus	Innovation in information Shift to online Outsourcing, third party, like cloud Connected devices	Global shocks (terrorist, climate, political) Business Resilience IoT Critical infrastructure State-sponsored cyber-attack-cyber war

Source Ernst and Young (2017)

6.1.3 Cyber Security Scenario in India

As per the CERT-In, Government of India (Indian Computer Emergency Response Team) in every 10 min at least 1 attack was reported in India in last six months in the year 2017. In the last three years, a total of 1.71 lakhs cybercrime was reported. According to Ministry of Electronics and Information Technology, central and state government Web sites were hacked at least 155 times in the year 2014 and 164 times in 2015 while the number rose to 199 times in 2016. According to NCRB 2016 report, it was 11,592 cases of reported cybercrime wherein Uttar Pradesh state topped with 2208 cases of reported cybercrime and was followed by Maharashtra. The major motives reported in the crime were in the area of financial gain, fraud, insult to modesty of women, sexual exploitation, blackmailing, plot motives, political motives, inciting hate crime, purchase of illegal drugs and casual disrepute. Leading IT security firm McAfee Labs reported 311 publicly disclosed security incidents and has stated that every minute 244 cases of cyber threats are reported to them. Delloite in its report stated cost of cybercrime can be 575$ billion per year. In urban areas, 99% of the children use Internet with weak passwords as per the survey made by Telenor India. Survey was conducted among 13 major cities in India among the children. More than 50% of the students in urban areas use passwords with only alphabets which as less than 8 digits. Such passwords are easy to hack and prone to cyber-attack. There is an urgent need to create awareness about password management in schools and colleges across the cities in India. According to the survey made by Kaspersky Lab, a research firm from Russia pointed out that only 47% across the globe use combination of upper and lower case in their passwords whereas only 64% use mixture of letters and numbers. Major security incidents listed by CERT-In in the year 2016 are as follows (Fig. 6.1).

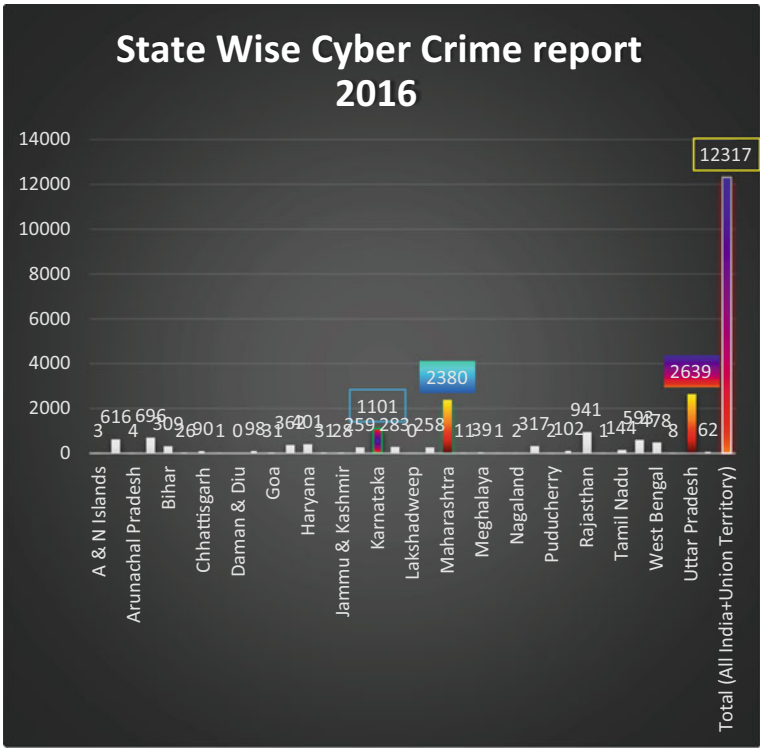

Fig. 6.1 State-wise crime report. *Source* NCRB, Government of India

From the above, we can clearly see that Uttar Pradesh has the highest number of cybercrime reported with 2639 in the year 2016, followed by Maharashtra with 2380 and Karnataka with 1101. The above reported cases are expected to go up with rapid growth of Internet penetration in the country. States like Telangana, Andhra Pradesh and Rajasthan will be the next IT hub of India, and the cybercrime is likely to go up in this area as well (Fig. 6.2).

As per the National Crime Report Bureau (NCRB), a maximum number of reported cases are from tier one cities in the country. Mumbai has the maximum number of reported cases of cybercrime in India which is followed by Bangalore, also called as the IT capital of India. Government of India is pushing hard to remove digital gap in rural areas by introducing new measures in promoting "Digital India" program. With such initiatives, cybercrime will go up in the coming years. Most of the reported cases of cybercrime in this city were on financial fraud, sexual exploitation, blackmailing, plot motives, political motives, inciting hate crime, purchase of illegal drugs and casual disrepute (Fig. 6.3).

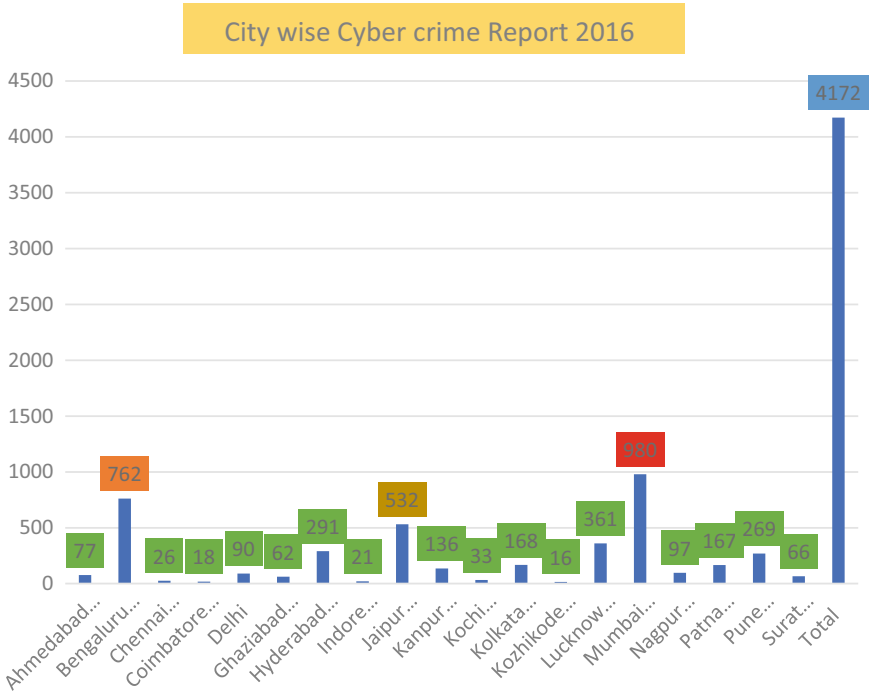

Fig. 6.2 City-wise cybercrime report 2016. *Source* NCRB, Govt. of India

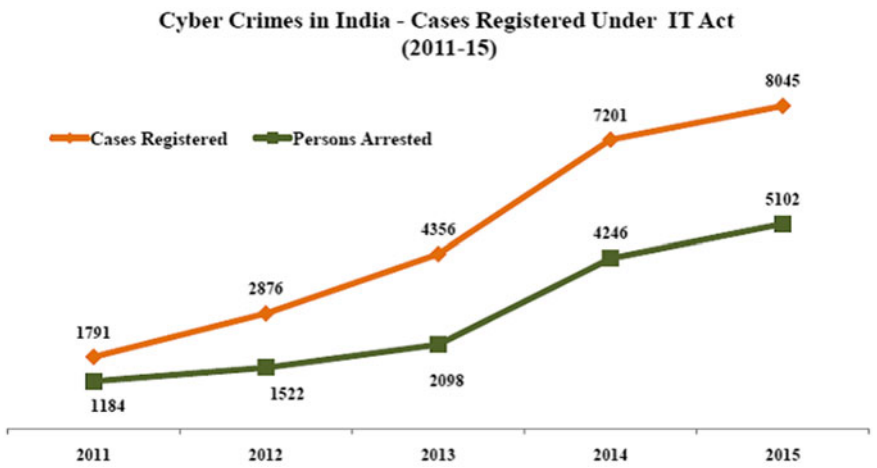

Fig. 6.3 Cybercrime graph. *Source* NCRB, Government of India

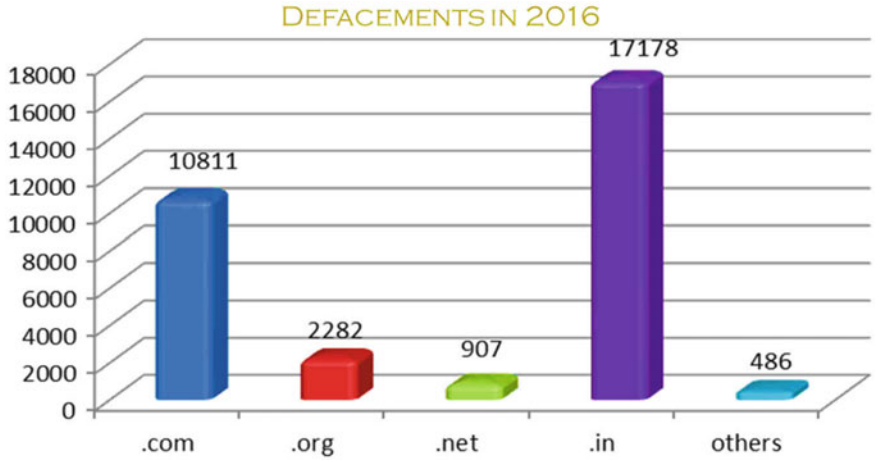

Fig. 6.4 Indian Web sites domain-wise defaced in the year 2016

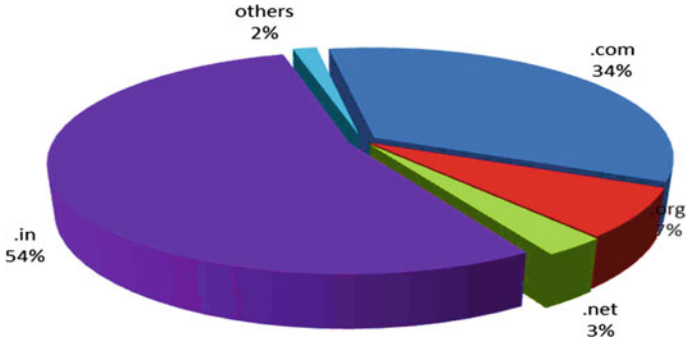

Fig. 6.5 Summary of Web sites defaced. *Source* NCRB, Govt. of India

From the year 2011–2015, number of reported cases of cybercrime increased rapidly. Surprisingly, number of persons arrested as per IT act under Indian panel code is quite low. In the year 2011, out of 1791 reported cases of cybercrime only 1184 were booked and arrested. However, in the year 2015, there were 8045 reported cases of cybercrime but only 5102 were arrested (Figs. 6.4 and 6.5).

Computer Emergency Response Team of India (CERT-In) has outlined and reported various cases of Cyber security incidents and noted domain-wise reported cases of attacks. From the above Table 6.2, we can figure out that Web site attack was mostly reported and is the highest number in the year 2016 followed by virus and malicious attack.

Table 6.2 Security incidents in the year 2016

Security incidents	2016
Phishing	757
Network scanning/probing	416
Virus/malicious code	13,371
Web site attack	31,664
Web site intrusion and malware propagation	1483
Others	2671
Total	50,362

Source NCRB, Govt. of India

Table 6.3 Dec 2017 reported cases

Domains	No. of defacements
.com	446
.in	1459
.net	23
.org	20
Others	14
Total	1962

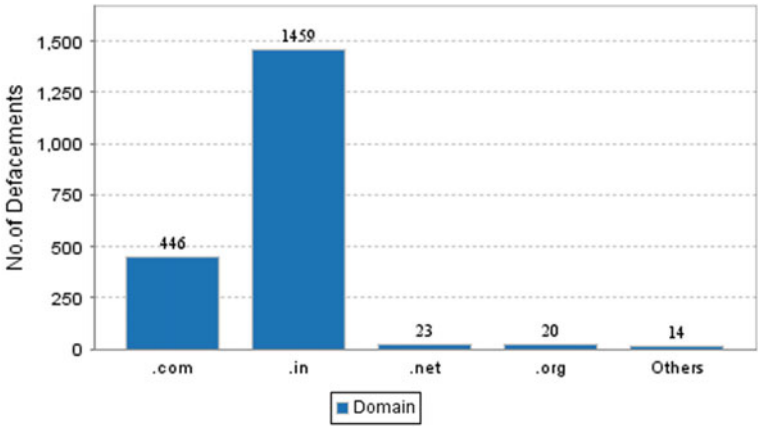

Fig. 6.6 Summary of domain-wise reported cases

Table 6.3 consists of latest report generated from CERT-In in the month of Dec 2017 (Fig. 6.6).

From the above table and summary, we can see reported cases of domain-specific defacements in the month of December 2017. We can see that .in domain has the

highest number of reported cases pertaining to Cyber security-related attacks. However, in the year 2016 as well we have seen most of the cases were reported from the same domain, i.e., 54% of the reported cases were from the .in domain. Cyber-attacks keep on growing because cyber-attacks are convenient, cheaper and involve smaller amount of risk than physical attacks. Cyber criminals require only a little expense like a computer and Internet connection. Unimpeded by topography and distance, it is difficult to identify and act against due to unidentified nature of the Internet. However, attack alongside IT systems are very striking, it is anticipated that the figure and complexity of cyber-attacks will keep increasing. With the series of initiatives undertaken by the government in empowering society by providing last mile network connectivity, cybercrime is going to rise certainly. Cyber security experts believe that malware is the key weapon that infects and carries out malicious attacks in the system. Malware refers to a group of harmful viruses, worm's attack that loads in the system and attacks the system without the permission of the owner. Malware includes viruses, worms, Trojan horse, spyware and software bug. System suffered from malware attack can damage end-user systems, servers, routers, switches and process control systems such as Supervisory Control and Data Acquisition (SCADA). Nowadays, malware is used to steal sensitive credit, debit card information by infecting in the system. Over the years, cybercrime has drastically increased. According to India's CERT-In (Computer Emergency Response Team), about 50,362 cyber security incidents were reported to the government in the year 2016. However, most of the incidents were fraud e-mails, Web site defacements, virus and denial of service was reported. As per the "2016 Cost of Data Breach Study": the total cost average of a data paid by the company increased by 9.5%. Government of India has taken certain strict cyber security initiatives discussed below for more full proof, open and robust measures are required to meet up the growing crime. As per the ASSOCHAM, India report, India will cross 3 lakhs by the year-end.

Major reported cases of cyber-attacks in India (Table 6.4).

6.1.4 Investment Required

Government of India should double the current investment in Cyber security initiatives by providing funded projects to institutes and research organizations in building open innovation culture. However, training man power is a foremost requirement and needs an immediate attention and investment. Government of India must create a nodal agency like CERT-In in each domain, for example Financial CERT-In, Defense CERT-Into counter to the external threats. Government of India spends the least amount for cyber security protection in comparison with other developing countries. Singapore has the highest budget allocation for building robust cyber security for the country. It spends 10% of IT budget for cyber security. As per 2014–15 report, IT department has spent 116 crores for Cyber security.

Table 6.4 Major cases reported in India

Company name	Type of attack
Reliance Jio	Unauthorized access to database
Star India	Unauthorized release of episodes of Game of Thrones leaked
Union Bank	Hackers managed to take bank's access codes by hacking into the server
Zomato	17 million user's database record was hacked
Renault India	Was hit by ransomware Wannacry global attack
IRCTC	Data theft from Web site
Yes Bank	Malware attack in ATMs and PoS machines
Hitachi Payment Systems	Malware attack of banks data
Bank of Maharashtra	Central server hacked
Reckitt Benckiser India	Hit by global ransomware attack

6.1.5 Future Threats and Trends

Rapid penetration of Internet across the globe brings a lot of challenges in cyber security. Future of Cyber security will be challenging to withstand with diverse and complicated attacks. As reported by many news articles, future of war will be fought in cyberspace between countries. Across the border, cyberterrorism will further grow with the advancement of technology. Such scenario requires new skill sets in data science and analytics. According to Gartner report, skills and organization will continuously change due to cyber security. In the world of AI, Big data, IoT protecting and securing will be a challenging effort. Cyber criminals usually look for data resources to get hold and steal important information. Platforms like plug and play will be prone to cyber-attacks in future. For example, Android Banker Trojan is a malicious application targeting users of Android phone specially banking apps to steal financial transactions details and passwords. Another latest threat comes from a newly observed malware named as "Mirai." It is a new variant of malware that targets IoT devices like printer, video camera, routers, smart TVs and smart devices. Business Email compromise (BEC) is a complicated attack targeting e-mail accounts of foreign suppliers to track hold of the financial transactions. Another trend pertaining to e-mail account is EAC (E-mail account Compromise) which is an associated scam of BEC. Ransomware was a huge success in the year 2017, wherein many organizations lost vital financial data from the system. It has targeted both human and technical weakness in an organization to deny vital data needed for the organizational functioning. Social media has billions of users all across the globe, and each of this shares personal details in public domain. Such details too can directly or indirectly help hackers in tracking details and stealing important information. As per CERT-In vulnerability warning in the Web site, Apple macOS Sierra version 10.13.3 was reported which could cause remote attacker to cause denial of service on the system.

6.1.6 Government Initiatives on Cyber Security

Government of India has formulated various policies and nodal centers to deal with cybercrimes and other related issues. Keeping in mind constant, complex cyber-attacks in the recent years, government has increased the cyber vigil across all domains. Currently, so-called cyber war takes place between countries to countries. Such attacks range from sensitive government and private services, defense installations, financial services and dedicated places. Government of India has directed law and enforcement agencies to strictly create nodal centers for protecting the major installations in various parts of the country.

6.1.7 NCS 2013-National Cyber Security Policy 2013

Indian government has formulated a national-wide Cyber Security Policy on July 2, 2013 to protect and legalized cyber-attacks to its citizens in the country under the ages of Ministry of Communication and Information Technology, Department of Electronics and Information Technology(MeitY). This policy aims to protect information infrastructure in cyberspace, reduce attacks, prevent attacks and respond to cyber threats and minimize damage during emergency attacks. The main broad objective of this policy is to create a robust ecosystem to secure the cyberspace of the country by providing layers of security and comply with the global cyber security standards and strengthen the cyber security framework in the country by providing round the clock cyber-surveillance to the country. It also aims to train 5 lakhs of cyber security expert to build robust cyber network and create a strong workforce to deal with the uncertainty. A strategy adopted by the National Cyber Security policy includes:

(a) Appointing national nodal agency and officer by encouraging private organizations to mutually chair and jointly regulate policies and develop robust cyber security policy for the country.
(b) Developing guarantee government regulation framework.
(c) Regulate wide open innovation standard in cyber security challenge.
(d) To create International Standard framework and spread awareness about the framework.
(e) Protecting electronic governance activities by implementing worldwide standard top practices and wider make use of public infrastructure space.
(f) Promoting cutting-edge research in educational institutes and private industry.
(g) To train human resource and create world-class man power in cyber security.
(h) To develop a robust information network for a full proof secure connectivity.
(i) Develop emergency and crisis management system.
(j) Collaborate with private firms to develop a mechanism of information sharing dedicated network to solve cyber problems.

Table 6.5 CERTN-in activities during year 2016

Activities	Year 2016
Security incidents handled	50,362
Security alerts issued	12
Advisories published	98
Vulnerability notes published	325
Training organized	11
Indian Web sites defacements tracked	31,664
Bot infected system tracked	10,020,947

In the year 2014, Prime Minister of India chaired and created a position called as "National Cyber Security Coordinator" to look after cyber security-related issues after a government site was hacked by infamous hacker group "Legion." Strong directive was ordered from the government to strengthen several financial IT systems in the government funded organizations.

6.1.8 CERT-in (Indian Computer Emergency Response Team)

To combat cyber-attack and prevent increase of such attacks in future, Government of India established a nodal agency, Information Technology Amendment Act 2008 of 70B section to perform following cyber security functions:

(a) To collect data, analyze it and spread the cyber incidents information.
(b) To calculate future attack and generate alerts on incidents of cyber security.
(c) To handle emergency and respond quickly to cyber breach incidents.
(d) Coordinate with cyber incident reaction activities.
(e) To issue comprehensive guidelines and spread awareness, prepare white paper on cyber security and reporting of cyber-attack incidents and provide training.

CERT-In during the year 2016 has the following incident handling reports (Table 6.5).

6.1.9 Cyber Swachhta Kendra-Botnet Cleaning and Malware Analysis Centre

In February 2017, Government of India launched "Botnet Cleaning and Malware Analysis Centre" for protection of desktop and solution of mobile security. It is operated by CERT-In, Government of India and is a part of Ministry of Electronics

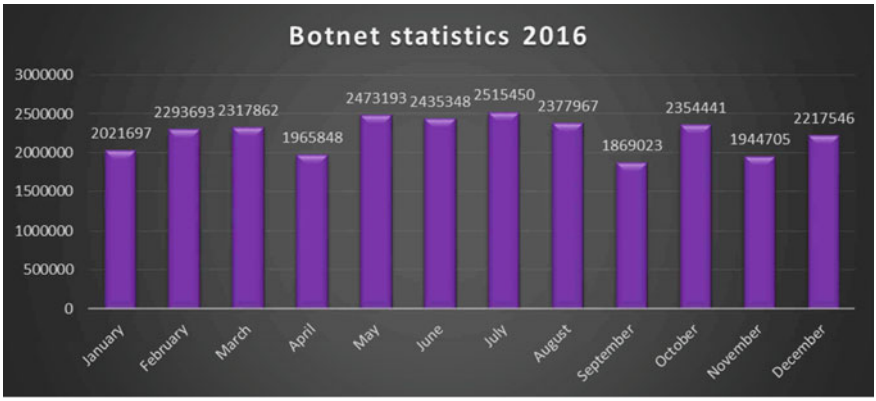

Fig. 6.7 Month-wise botnet 2016. *Source* NCRB

and Information Technology (MeitY). This application will become aware of botnet malware infections and avert further infection by clearing out the current infection and notifying the end user and create awareness. The Cyber Swachhta Kendra will also collaborate with industry and academic institution to detect malware infections and also collaborate with network service provider to remove infection and generate end-user awareness. Government has introduced certain security and protective tools to enhance the unauthorized access of data. Some of them are as follows.

(a) USB Pratirodh—An application developed to control unauthorized access of removable USB device like external pen drive, hard drive and USB compatible storage space system.
(b) Samvid—It is application-based software for desktop which is used for whitelisting windows operating system from running suspicious application.
(c) M-Kavach—It is a device for Android mobile devices to protect from malware, misuse of Wi-Fi, Bluetooth resources, stolen mobile devices, spam messages, unsolicited incoming calls.
(d) Browser JSGuard—It is a browser expansion tool which informs and protects from infectious html and web-based scrip-related attack made through browser extension. This particular tool reports the user and alerts the user as well.

Figure. 6.7 shows the monthly wise botnet infected systems tracked in India in the year 2016.

From the above figure, we can see month-wise botnet report generated by CERT-In during the year 2016. July 2016 has the highest number of detected malware amounting to 251,540 and followed by May 2016 with 2473193. The above report shows only the detected botnet system of that particular year.

6.1.10 National Informatics Centre (NIC)

NIC is a premier organization in the country that supports central, state, union territories, districts and government bodies in information and communication technology by providing e-government services. NIC is a nodal center set up by the Ministry of Electronics and Information Technology, Government. of India. It offers telecommunication networking services like LAN gateways and Wi-Fi gateways.

6.1.11 NISAP—National Information Security Assurance Program

NISAP is a national awareness program to highlight the importance of securing data and creating infrastructure. It was a pilot program to create awareness among the citizens and organizations about the cybercrime issues. MietY in collaboration with CERT-In started this program across the country to create awareness and generate enthusiasm among the citizens.

6.1.12 Indo-US Cyber Security Forum (IUSCSF)

India and USA jointly set up a forum in the year 2011 to cater to the needs of the cyber security. The focus was in information sharing and to raise awareness about the budding threats in cyberspace and set up anti-boot alliance along with Confederation of Indian Industry (CII). In addition, India and America agreed on joint research and development in the areas of cyber security by setting up anti-spasm research.

6.1.13 International Partnerships and Agreements

The focus of Government of India currently is to strengthen international partnerships to deal cyber security issues effectively. Government has recently signed Memorandum of Understanding (MoU) between CERT-In team and CERT-UK, Information security center Uzbekistan and Vietnam.

6.1.14 Recommendations

Government of India's "Digital India" program aimed at empowering citizens with seamless connectivity, expanding access and improving the lives of its citizens is

incomplete without providing a robust cyber security protection. As the Cyber security continues to grow rapidly, Government of India must update the Cyber security policy 2013 and prioritize certain policies that need immediate attention. In the last five years since the implementation of Cyber Security Policy 2013, India's cyber security landscape has witnessed dramatic changes with various sophisticated attacks. Government of India should immediately formulate a comprehensive and robust Cyber security policy and institutional framework to address the country's digital safety needs. Government of India should take steps to build highly skilled Cyber security workforce and professionals in the next five years and create a robust digital infrastructure for skill development and training facility to students. To promote greater accountability, Government of India should implement ethical hacking in schools and colleges and create awareness among them. Some of the immediate steps government should take are outlined below:

1. Implement the existing Cyber security policy 2013 in a time bound manner without further delay.
2. Update Cyber Security Policy 2013.
3. Create a robust digital cyber-physical network for robust monitoring and networking with the system.
4. Public–private partnership and collaborative engagement through technical, operational, research and development for protecting the cyberspace.
5. Create greater civil-military cooperation on Cyber security.
6. State-wise creation of cyber security center to monitor cybercrime.
7. Cooperation between government and education institutes in information sharing, research and development activities.
8. Government should conduct continuous workshops, awareness programs and training programs to create awareness among the young generation.
9. Government should promote Cyber security knowledge through radio, TV aids, webinars, online contests, promotional on social media, newspapers, banners, posters, conference and videos on relevant topics on cyber security.
10. Develop Cyber security infrastructure in each state and provide training to lakhs of youths and employ them in various places in the country.
11. Speed trail of cybercriminal under the law, it will send a strong message for the young generation not to venture into such acts in future.
12. Keeping in mind privacy of its citizens, government should maintain strict guidelines to private operators.
13. International collaboration among countries to counter cyberterrorist attacks.
14. Government of India should make white papers for the protection of data.
15. Create robust information sharing within the states of the country.
16. Create counter terrorism cyber cells in the country.
17. Set up Cyber security cell in each district administration in the country.
18. Set up fast track cyber security court for swift delivery of service to the people as per Indian law.
19. Monitor Cyber security centers regularly.

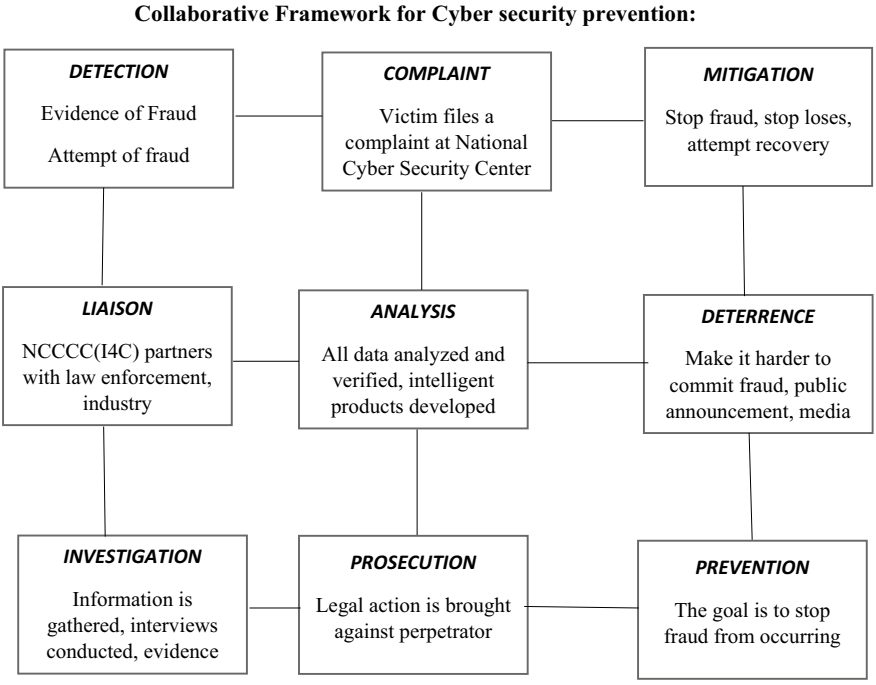

Fig. 6.8 Collaborative framework for Cyber security prevention

20. Implement emergency crisis management framework to enable organizations to response swiftly and withstand future attacks (Fig. 6.8).

Thousands of people in India are victims of cybercrime every year. Only ample number of reported cases are booked under the law while many cases remain unanswered. Detection of cybercrime is the first priority and is an eye opener of larger crime. Reported cases of cybercrime victim then lodge formal or online complain to the law enforcement agency. Here, the victim is advised to document in detail to support his evidence. Apart from reporting the crime online, victim takes the steps to mitigate further loses by approaching banks, credit card companies to block or freeze the account and recover loses by legal means if such policy exists within the system. Government of India should set up I4C (Indian Internet crime complaint Center) like the USA to take care of the online complain. This organization will review and access the victims complain and address immediate measures to highlight the level of damage and alert potential users. It will also analyze the data and circulate to all states in the country to take immediate measures to protect potential victims. Information sharing will play a key role in enhancing cyber security in the country. Then, the next steps would be to circulate in print news, social media to spread awareness in the country and stop further attacks and damage. Prevention and deterrence of future attack are very important in the present context to protect

further escalation and repeated attacks. Prosecution of the attacker be made public and without any bias. Booked victim be made to pay the price by imposing heavy penalty and prosecute under the law of the land. Proper and transparent investigation be undertaken without delay. Government of India should make sure that the Web sites are surfed with a secured https enabled link as it indicates a secured network. Good start-up environment and funding should be introduced by the government to promote cyber security start-ups in India. Cyber security is a global phenomenon and is rapidly growing with each day. India needs to stand tall to withstand future cyber security challenges. AI backed Cyber security protection tool will soon take over from traditional protection methods. Cyber Security Policy can be challenging because of its intangible nature, social technical dependence, ambiguous impact and contested nature of fighting cyber security. Slowly our society is turning into a cyber-physical society having dependence on Information and Communication Technology (ICT) across all aspects of our daily lives which makes it very important. Government should emphasize on Big data analytics and cloud computing techniques to protect cyber breaches. In addition, citizens of the country should be aware of the latest trends and threats in cyberspace. Hence more and more awareness programs must be encouraged within the country, state and district level.

References

Agarwal, S. (2016). IT Minister orders measures to strengthen India's cyber security. *The Economic Times*. Retrieved from http://economictimes.indiatimes.com/articleshow/55963728.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst. Accessed on 13 January 2018

CISCO. (2011). The internet of things: How the next evolution of the internet is changing everything. Retrived from https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. Accessed on January 2018.

Datta, S. (2014). India's cyber protection pushes ahead. *Hindustan Times.* Retrieved from https://www.hindustantimes.com/india/india-s-cyber-protection-body-pushes-ahead/story-4xa9tjaz6ycfDpVg95YqPL.html. Accessed on February 25, 2018.

EY. (2016). *Path to cyber resilience: Sense, resist react, global information security survey 2016–17 Indian report*. EY. Retrieved from http://www.ey.com/in/en/services/advisory/ey-global-information-security-survey-2016-2017-india-report. Accessed on February 2018.

Hazel, K., & Raghav Rao, H. (2017). Cyber-rumor sharing under a homeland security threat in the context of government Internet surveillance: The case of South-North Korea conflict. *Government Information Quarterly, 34*(2), 307–316.

IDC. (2014). *The digital universe of opportunities: Rich data and the Increasing values of the Internet of Things*. EMC Digital Universe with the Research and Analysis. Retrieved from https://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm. Accessed on January 16, 2018.

Internet and Mobile Association of India. (2018). Retrieved from https://www.iamai.in/. Accessed on December 2018.

Kumar, A. (2016). *As India gears up for cyber security challenges, threats are multiplying*. Security Intelligence IBM. Retrieved from https://securityintelligence.com/as-india-gears-up-for-cybersecurity-challenges-threats-are-multiplying/. Accessed on January 12, 2018.

PIB. (2014). *Digital India—A program to transform India into a digital empowered society and knowledge economy*. Press Information Bureau, Government of India. Retrieved from http://pib.nic.in/newsite/PrintRelease.aspx?relid=108926. Accessed on January 15, 2018.

Sukumar, A. M. (2016). Upgrading India's cyber security architecture. *The Hindu*. Retrieved from http://www.thehindu.com/opinion/columns/upgrading-indias-cyber-security-architecture/article8327987.ece. Accessed on January 20, 2018.

US. (2016). 2016 *Internet crime report*. FBI IC3. Retrieved from https://www.ic3.gov/default.aspx. Accessed on January 10, 2018.