HOW DIGITAL INDIA IS TACKLING CYBERCRIME?

Ruma Saha

Assistant Professor,

Adamas University, Department of Journalism and Mass Communication

Email - ruma.saha.kolkata@gmail.com, Phone – 9433457655

Abstract

Cybercrime has extended its prowess throughout the world since its inception. India did not face the severity of its attack previously like its western counterpart as technology was still in its developing stage to transform the nation to digitally connected economy. Since 2014 onward India also advanced its footstep for more tech savvy nation where the financial transactions, records and government data are now stored on digital platform. India is moving towards the concept of e-governance and thereby opening the gateway to new form of enemies in the silhouette of cybercrime. According to IAMAI report by 2017 India is having more than 300 million internet user. [2] The penetration rate of Internet was 34.8% in 2016. [1] This shows that a huge number of people and huge amount of information are vulnerable in this cyber space. But the question arise are we still vulnerable when so many anti-virus company thrives in thismarket. Technology has upgraded and government data is also protected under strict surveillancebut still we face the crisis like Wanna Cry. This article focuses on how India is capable enough to tackle cyber-crime in its newly transformed digitally connected economy.

Keywords: Cyber-crime, cyber security, Digital India

Introduction

Cybercrime is a crime which involves computer as the object or tool of the crime (phishing, hacking, identity theft). Cyber criminals use computer technology to get access to personal information as well as business or trade secrets, or use the internet for malicious purposes. [3] Cyber-crime therefore signifies occurrence of harmful behaviour that is related to computer. It has no specific reference in law but the concept is invented by media (Wall, 2003). Internet has impacted upon criminal or harmful activity in three main way. This classification has been done

to distinguish cyber-crime from other crime. Firstly, internet is a vehicle of communication that assist in sustaining existing harmful activity like drug trafficking, hate speech, bomb talk,stalking and many more. Secondly, internet has created transnational environment that provide new platform for harmful activity like paedophile incident, fraud etc. Thirdly, the internet has created crime like unauthorized access to imagery, music, video, software tools etc. It has impacted both private individuals and business houses. Now the policy makers are to decide which policy is suitable for each of these crimes categorized under different level of cyber-crime.[4]

The first ARPANET link was established between the University of California, Los Angeles (UCLA) and the Stanford Research Institute in 1969. [3] The first words that they send through this network was "LOGIN". At that time no one could think that internet would gain such prominence that about 48% of the world's population uses the Internet. [3] This has increased the complicacies of cyber-attack many fold with its impact on half of the world population. Therefore a strong policy based on cyber ethics is required to be implemented by government of every country and also by transnational organisations like UN.

From mid-1990s onward government of India has taken e-government initiative to provide better service to the citizen. The major ICT initiatives of the government included some major projects such as railway computerization, land record computerization etc. that focused mainly on the development of information technology and systems. [5] Later on many states started implementing e-governance project to give electronic service to its citizen.

E-governance project could not make desired impact due to its limited features. E-governance project was characterised by isolated and less interactive systems, which posed as major drawback in adoption of this e-governance in broad spectrum of governance. They clearly pointed towards the need for a more comprehensive planning. Moreover, proper infrastructure is to be built in order to establish a more connected programme. As a result, government of India started the digital India programme to promote inclusive growth which covers electronic services, products, devices, job opportunities as well as transfer the entire ecosystem of public services through the use of information technology to a digital platform. [5]

In recent times, government's ambitious projects of Digital India and smart cities initiatives have already earned enough attention from heads of technology giant. But they are concerned about

the security policy to be implemented by government of India to enhance cyber security as security breaching is a regular feature now-a-days. [6] The report also suggest that the integrated digital footprint created by Digital India and digital cities will bring increasing and alarming demand for resources to defend against the threat at various level and entry point of the new system. Digital India and smart cities will create social and economic opportunities. [6] The increasing synchronization of existing digital data and processes within government departments will require maximum security. But critical data flow is to be left uninterrupted even in this high threatening environment. [6]

This article is devoted to study the current scenario of cyber security in Digital India. Also to find out how digital India is tackling cyber-crime. Issues of cyber ethics play a vital role in deciding policies made by policy makers.

Present Scenario of Cyber-crime in Digital India

Cyberspace touches every part of our daily life through wireless signals, broadband networks, local networks and even the massive grid that power our country. To create a strong defence system against cyber-attack would require combined effort from both public and private sectors. Combined effort is required to develop new technologies and new approaches for maintaining real-time protection of their individual networks. Now a days as most of the business are using open source due to cost factor the cyber threat becomes more lethal for business groups. [9] Since 2014 Indian government headed by Prime Minister Narendra Modi has taken several transformative initiatives like Adhaar, De-monetization and Digital India to add speed to India's transition from an analog to a digital economy. This is quite admirable goal and if executed properly it can jumpstart economic growth of India and creates crores of job opportunities. This goal will remain unattainable if India does not improve cyber security infrastructure. [10] Despite being IT powerhouse India's cyber security preparedness and infrastructure is far below the required level.

Recently two developments in cyber world in past few years made this scenario of unpreparedness even more dangerous. The first major development was the discovery of malicious computer worm called "Stuxnet." A group of cyber researcher had found it in 2010. Stuxnet was created to target industrial computer system. Stuxnet was different from other virus

in a way that it targeted programmable logic controller (PLC) which are not connected to the internet and previously thought to be safe from hacking. Stuxnet showed that many elements of any country's infrastructure such as water treatment facilities, hospital systems, dams, electric grids, factory assembly lines, power plant that uses PLC system and supervisory control and data acquisition system are also under cyber threat even though they are not connected to internet. It is high time for India to fortify its critical infrastructure. [10]

Second development in cyber space was the advent of another sophisticated malware named Advanced Persistent Threats (APT) in 2013. These malware perform in a different waycompared to any virus. Through this malware hacker aimed at data theft and espionage. Afterinfecting the target the malware use sophisticated root kit technique to disguise them. Theyconnect to control servers and command on the internet. They can export data as well as takenew instruction. This malware can remain undetected for months or even years while slowly collecting valuable data from victim's network. All the recent data theft incidents like Anthem, Target, Office of Personnel Management (OPM), Sony were victims of this malware attack. Government of India should think seriously regarding cyber security policy of the country. [10]

A study made by Assocham-PwC revealed that India has witnessed a 350per cent rise in cyber-crime from 2011 to 2014. [11] With the spread of smartphone and internet India has emerged as one of the favourite countries to attack among cyber criminals. The Indian Computer Emergency Response Team (CERT-In) has also reported in a study conducted by them under title "Protecting interconnected systems in the cyber era" that in 2015 a rise in number of incidents of cyber-attack could be noted at around 50000. [11]

Therefore, with increase in the usage of consumer technology (CT) as well as information and operational technology (OT) in critical infrastructure the threat situation is heightened. The study further noted that these vital elements have been the choice of target for attackers because they are aware of the impact of disrupting the routine way of life. [11] In USA an increase of 50% is noted in cyber-crime incident report against its critical infrastructure from 2012 to 2015. Victims are not only private individuals but also government and big business houses. [11]

Online news sites have recently reported in September 2016 on data breach of India's top secret file due to cyber-attack. The top secret "Scorpene" submarine program was published online and this data breach has brought the issue of cyber security of India into newspaper headlines. The

cyber security firm Symantec have mentioned in its blog post on 2016 that it had traced cyber security breaches of several Indian organisations by cyber espionage group called Suckfly. [12] According to Symantec this cyber espionage group has targeted government organisations, financial institutions, large vendors to stock exchange, e-commerce companies etc. Based on the targets that the group penetrated Symantec has speculated that the espionage was targeted at disrupting the country's economic infrastructure. [12] The government authority has neither denied nor accepted of being victim of such data breach. [12]

Recently in May, 2017 world was send to edge even without losing much money as intended from the victims by a ransomware named WannaCry. Impact was heavily felt in UK where National Health Service was hard hit by stalling surgeries, calling back ambulances etc. This led the cyber experts throughout the world to think about the real time impact like this. All of us live in a digital world where destructive effect is hard to stop. [13] Researchers have observed that WannaCry is a program mainly targeting Microsoft Windows operating systems. The hacker uses this ransomware to take control of victim's computer and lock the data until the victim pay in return. The hacker demanded payment of $300 to $600 using Bitcoins. Microsoft has releasedcyber security to overcome this vulnerability but that will not be applicable for any pirated software. Cyber security experts were of opinion that outspread of attack would be high in India as majority of the computers are working on pirated software. [14] Some newspapers reported that Ministry of Home Affairs source had informed that Government of India had ordered to shutdown the service of some ATM outlets all over the country as preventive measures against the cyber-attack.[15] As far as the effects are concerned IT minister of India Ravi Shankar Prasad said that India was not affected much by ransomware WannaCry. [15] He added that ransomware WannaCry had partially affected Kerala and Andhra Pradesh. [15] Some newspaper reported of ransomware attack in parts of West Bengal. [14] Government is keeping close eye to the situation as well as improving its security system. Indian Computer Emergency Response Team (CERT-In) has recently come out with list of preventive measures to protect networksfrom global ransomware attack. [15]

Reserve Bank of India (RBI) has directed the banks to update the software in their ATM machines to avoid ransomware attack. [14] The attack has crippled more than 200000 computers throughout the world and affected hospital, banks, government agencies in several countries.

[14] Researchers have come up with new term "cyber terrorism." Cyber terrorism is the

convergence of terrorism and cyber space. It is the use of internet to shut down critical infrastructure (electricity, bank, organisations, transport) with the purpose of coercing the people orintimidate a government. A hostile nation can exploit using these tools to penetrate poorly secured computer network and disrupt critical functions. [16]

Cyber security and policies in Digital India

What is cyber ethics?

Information Technology plays a pivotal role in every sphere in business, industry, government, medicine, entertainment, education and in society at large. The economic and social benefit gained from it hardly needs any explanation. Information technology too has negative implication in our society. This poses some problems related to ethics and generally contains three main types of ethical issues: personal privacy, access right and harmful actions. [7]

The increase in business transaction on intangible assets like Intellectual Property made cyber space an important commercial sphere. Therefore in order to extend this business, a secure cyber sphere is required. To protect intellectual property rights in online platform a strong regulatory agenda would be set and it will produce many technical methods of enforcement. Internet has turn out to become the media of the people as the internet has spread fast which initiated achange in press environment that is centered on mass media. Unlike established press there are no editors in internet; People produce content themselves and circulate it. This direct way ofcommunication over internet created many social debates. Hence, cyberspace content demandsin future a reconciliation of two views - freedom of expression and concern for community standards. [17]

Cyber laws in India:

1. Information and Technology Act, 2000 - The Information and Technology Act seeks to protect the technology and cyber space by defining crimes, laying down procedures for investigation, prescribing punishments as well as forming regulatory authority. Many cyber-crimes have been brought within the definition of traditional crimes too by means of amendment

to the Indian Penal Code, 1860. The Evidence Act, 1872 and Banker's Book Evidence Act, 1891 was amended to facilitate collection of evidence in fighting cyber-crimes. The IT act itself was amended in 2008 to adapt with changing cyber space. [17]

2. National Cyber security Policy 2013 – The Act was formulate to provide cyber security to growing IT industry in India but its implementation is not successfully done yet. Important features of this Act are as follows:

i. To build secure and resilient cyber space.

ii. Creating a secure cyber ecosystem, generate trust in IT transactions.

iii. 24 x 7 National Critical Information Infrastructure Protection Center (NCIIPC).

iv. Indigenous technological solutions is to be set up,

v. Testing of ICT products and certifying them. Validated products,

vi. Creating workforce of 500,000 professionals in the field,

vii. Fiscal Benefits for businessman who accepts standard IT practices, etc. [17]

Future of cyber security in Digital India:

The government takes initiative to conducted several awareness and training programmes on cyber-crimes for law enforcement body. Training is also given on the use of cyber forensic software packages and other associated procedures to collect electronic evidence from crime scene. [17] The initiative to provide cyber security and related projects are quite less in numbers. Even if there are some proposal for projects but that remained in papers only. India has launched e-surveillance projects like National Intelligence Grid (NATGRID), Central Monitoring System (CMS), Internet Spy System Network and Traffic Analysis System (NETRA) of India etc. But none of them are governed by any legal framework neither they were under Parliamentary Scrutiny. Thus, these projects are violation of civil liberties protection in cyberspace. Government has formed National Informatics Centre (NIC) to provide network backbone to manage IT services, E-GOV initiatives to state and central government. To counter cyber-crime a coordination is required from different agencies working under Ministry of Home Affairs and under Ministry of Communications and Information Technology. Apart from Central Bureau of Investigation, The Intelligence Bureau, state police organizations and other specialised organizations such as the National Police Academy, there are few agencies of government which

also work for tackling cyber-crime. To name few of them are : National Information Board (NIB) , National Crisis Management Committee (NCMC), National Security Council Secretariat (NSCS), Department of Information Technology (DIT), Department of Telecommunications (DoT), National Cyber Response Centre – Indian Computer Emergency Response Team (CERTIn), National Information Infrastructure Protection Centre (NIIPC), National Disaster Management of Authority (NDMA), Standardization, Testing and Quality Certification (STQC) Directorate, The Cyber Regulations Appellate Tribunal. [17]

Inter-governmental organisation and initiatives:

Various intergovernmental organisations have taken initiatives to address the issue of cyber-crime at policy level.

Council Of Europe - Council of Europe aimed at protecting societies throughout the world from the threat of cyber-crime through Convention on Cybercrime held at Budapest in November, 2001. It was the first international treaty to address the problem of cyber-crimes that is done using internet and computers. Budapest Convention entered into force from July 2004. [18]

Internet Governance Forum (IGF) – It was established in 2006 by the World Summit on the Information Society to bring people together from different stakeholders groups for discussion on public issues related to internet. United Nation played a vital role in establishment of IGF. [19]

United Nation – The International Telecommunication Union (ITU) is the specialized wings of UN deals with information and communication of the world. They also deal with adoption of international standards to ensure uninterrupted global communications and flexibility for next generation networks. They also work for building confidence and ensure secure ICT usage. [17]

Meridian Process - The Meridian Process has set its goal in providing Governments throughout the world a platform or means to discuss on how to work together at the policy level on matters of Critical Information Infrastructure Protection (CIIP). By holding annual conference the organisation tries to build trust and establish international relations within the member countries as well as provide opportunity for sharing best practices from the world. [20]

NETmundial Conference - Brazil had hosted NETmundial – Global Multi-stakeholder Meeting on the Future of Internet Governance in 2014. The meeting was held in collaboration of Brazilian Internet Steering Committee and /1Net. It is a forum that gathers international entities of various stakeholders involved with e-governance. This meeting mainly focused on elaboration of principles of Internet governance and the proposed a roadmap for future development of this ecosystem. [8]

Conclusion

The increase in the number of internet users around the world makes data security as well as its proper management very important for future growth and prosperity. The main concern is with the unauthorized people who are trying to access remote services and disrupt the system. It has become our responsibility for our own cyber security. Simple steps are to be followed to stay in secured cyber space like installing antivirus software, personal firewall and update it time to time. Also it is advisory to archive all security logs. Moreover access should be restricted to sensitive data and has to be password secured. Above all more cyber literacy related to cyber security has to be enhanced. Government can also utilise specializations of private sectors to tackle problems of cyber security and promote more PPP projects for having secured Digital India.

Reference:

1. http://www.internetlivestats.com/internet-users/india/ (Accessed on June 12,2017)

2. http://www.iamai.in/media/details/3658, (Accessed on June 12,2017)

3. Dave, D. P. H. S. S., & Patel, M. P. (2017). Organized Cyber-Crime and the State of User Privacy.

4. Wall, D. (Ed.). (2003).Crime and the Internet.

5. Turka, S. K., & Singh, G. (2016). Issues and Challenges of Digital India Programme in the Current Scenario. Academic Discourse, *5*(2), 76-81.

6. http://www.financialexpress.com/industry/technology/security-in-the-age-of-digital-india/91341/ (Accessed on June 13,2017)

7. Gunarto, H. (2014). Ethical issues in cyberspace and IT society. Ritsumeika Asia Pacific University.

8. http://netmundial.br/about/, (Accessed on June 15,2017)

9. http://digitalcreed.in/cyber-security-critical-for-digital-india-success/ , (Accessed on June 14)

10. http://timesofindia.indiatimes.com/people/opinion-digital-india-requires-cyber-security-investment/articleshow/57847654.cms, (Accessed on June 14,2017)

11. http://kenes-exhibitions.com/cybersecurity/blog/digital-india-cyber-security-threat/, (Accessed on June 14,2017)

12. https://thewire.in/67398/india-is-unprepared-for-future-cyber-attacks/, (Accessed on June 14,2017)

13. http://indianexpress.com/article/opinion/wannacry-attack-ransomeware-virus-patch-is-india-ready-for-the-perils-of-a-hyper-digital-world-4656925/, (Accessed on June 15,2017)

14. http://indiatoday.intoday.in/story/wanna-cry-ransomwares-impact-in-india-may-go-under-reported/1/954798.html, (Accessed on June 15,2017)

15. http://indiatoday.intoday.in/story/atms-shut-down-india-wanna-cry-ransomware-attack/1/954284.html, (Accessed on June 15,2017)

16. https://en.wikipedia.org/wiki/Cyberterrorism , (Accessed on June 15,2017)

17. http://www.insightsonindia.com/2014/11/25/cyber-security-related-issues-comprehensive-coverage/, (Accessed on June 15,2017)

18. https://en.wikipedia.org/wiki/Convention_on_Cybercrime, (Accessed on June 15,2017)

19. http://www.intgovforum.org/multilingual/content/about-igf-faqs, (Accessed on June15,2017)

20. https://www.meridianprocess.org/, (Accessed on June 15,2017)