Impact Factor 3.025

ISSN 2349-638x

Refereed And Indexed Journal

AAYUSHI INTERNATIONAL INTERDISCIPLINARY RESEARCH JOURNAL (AIIRJ)

Monthly Publish Journal

VOL-IV ISSUE-V MAY 2017

Address
· Vikram Nagar, Boudhi Chouk, Latur.
· Tq. Latur, Dis. Latur 413512 (MS.)
· (+91) 9922455749, (+91) 9158387437

Email
· aiirjpramod@gmail.com
· aayushijournal@gmail.com

Website
· www.aiirjournal.com

CHIEF EDITOR – PRAMOD PRAKASHRAO TANDALE

Cyber Security and India

Mrs. Reena Devi,
Assistant Professor,
Pt. Sita Ram Shanti B.Ed College, Bhiwani
reena84sheoren@gmail.com

Abstract*:*

Information Technology on one hand has been one of the leading drivers of globalization and on the other it has also become one of its major victims. Nowadays cyber crime is the most concerning issue for all developed and developing countries, because it harms governmental confidential data as well as people in daily life transactions. So it is the need of the hour to come up with better and effective cyber security measures. In this paper we have focussed on the existing cyber security infrastructure and the growing need to come up with changes that would be more efficient to deal with issues of increasing cybercrimes.

1. Introduction*:*

No other medium in the history of humankind has had such potential and global reach as the Internet. It has indeed been a major opportunity as well as a security nightmare since cyber- attacks can be a lot more than just inconvenient. So there is an implied need for cyber-security infrastructure. **Cyber-security**[1] may be defined as all measures aimed at protecting computer networks and digitized data from cyber threats, including cybercrimes and other harmful activities, which may bring harm to a large number of individuals or hold a risk significant material damage. The cyber security threats emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike. Their effects carry significant risk for public safety, security of nation and the stability of the globally linked economy as a whole. The origin of a disruption, the identity of perpetrator or the motivation for it can be difficult to ascertain and the act can take place from virtually anywhere. These attributes facilitate the use of Information Technology for disruptive activities.

2. India's Cyber Vulnerabilities:

India has carried a niche for itself in the IT Sector. She has already brought sectors like income tax, passports" visa under the realm of e -governance. Sectors like police and judiciary are to follow. The travel sector is also heavily reliant on this. Most of the Indian banks have gone on full-scale computerization. This has also brought in concepts of e-commerce and e-banking. To create havoc in the country these are lucrative targets to paralyze the economic and financial institutions and these are actually being targeted. Today, the necessity of strong cybersecurity measures is self evident. A proliferation of cyber attacks is causing increasing damage to companies, governments and individuals. Yahoo's disclosure of a massive breach is still making headlines. In the recent past also we have experienced a lot for example, the series of **bomb attacks of 2006-07**[2] across several prominent Indian cities, one of the most audacious **attacks of 26/11**[3], the espionage campaign by Ghost Net, Chinese espionage activities [against DRDO in March 2012 and Indian Navy's Eastern Command in June 2012] and attack on Indira Gandhi International Airport network and several other incidents of cyber terrorism illustrate how the terrorist-handlers are now exploiting technology to

cause terror and massive destruction. Not only terrorism rather cybercrimes like cyber obscenity, child pornography, stalking, financial cybercrimes, etc. still cover large sections of newspapers. The cases registered under the IT act grew by more than 350% from 2011 to 2015. There was almost a 70% increase in the number of cyber crimes under the IT act between 2013 and 2014. The cases registered under the IPC increased by more than 7 times during the period between 2011 and 2015. Similar trend is observed in the number of persons arrested.

The data [4] here shows that there has been an increase in threats and attacks in quantum leaps:

Table : Growth in select cybersecurity threats, 2006-2007 to 2014-2015

S.No.	Event	2006-07	2014- 15
1.	Security Incidents Handled	552	130338
2.	Security Alerts Issued	48	13
3.	Advisories Published	50	69
4.	Vulnerability Notes Published	138	290
5.	Indian Website Defaced	5211	25037
6.	Open Proxy Servers Tracked	1837	2408
7.	BOT Infected Systems	No Data Generated	7728408

The Government agencies need to set an example in the development and use of secure computer and communication networks. There is a need for priority action to strengthen the security of the Government IT infrastructure to facilitate faster and efficient information flow between various user agencies within the Government as well as effective interface with users outside the Government. In order to meet the upcoming challenges in securing the Government IT infrastructure, adequate attention should be paid to the use of appropriate technology and applications and development of suitable - Information security policies and guidelines.

3.Cyber security Infrastructure*:*

We have seen that India is rapidly moving towards a digital ecosystem. The number of connected devices is only increasing and the Internet is penetrating the remotest of areas, but have we covered all our bases? There are huge gaps in India's cyber-security infrastructure. India might be ready for a digital future but is it truly prepared to handle the security risks that tag along? To get answers to these questions it is important to know the existing cyber security infrastructure.

3.1 The Information Technology Act of 2000*:*

The road to developing a framework for cyber-security in India has been a slow and torturous process. In the year 2000, India enacted its first law on Information Technology namely, the Information Technology Act, 2000. The IT Act, 2000 is based on the Model law of Ecommerce adopted by **UNCITRAL** in 1996.While the Information Technology Act, 2000 [5] had rudimentary clauses for protecting data, there was no comprehensive clause that looked at cyber-security per se from a statutory perspective as India was still at a nascent stage of its journey of embracing the

Internet, and the computerisation of large government networks and processes was just beginning. It was passed to provide legal recognition for transactions carried out by means of electronic communication i.e. the Act initially was actually drawn up to protect the business interests of the IT-enabled services (**ITES**) industry. The original IT Act of 2000 appointed the **CCA**[6] as the major point-person for most data security related procedures and functions, emphasising data security, rather than cyber-security. In fact, the Act did not mention cyber-security even once, and had limited scope in looking at the issue of security. Clearly, the initial version of the IT Act failed to fully appreciate the power of technology and its impact in the years to come. In recognition of the rise in cyber vulnerabilities, threats and attacks and the emergence of new threats, the statutory framework was reworked and then came the **Information Technology (amendment) Act, 2008(Act 10 of 2009)** with significant additions to the previous Act , with the aim of establishing a national cyber-security policy framework.

3.1.1 IT (Amendment) Act, 2008 [7]**:**

The IT (Amendment) Act, 2008 has brought marked changes in the IT Act, 2000 on several counts. Some of these that are relevant here are further discussed briefly.

a) ***New cybercrimes as offences under amended Act*-**Many cybercrimes for which no express provisions existed in the IT Act, 2000 now stand included by the IT (Amendment) Act, 2008. Sending of offensive or false messages (**s.66A**), receiving stolen computer resource (**s. 66B**), identity theft (**s. 66C**), cheating by personating (**s. 66D**), violation of privacy (**s. 66E**). A new offence of Cyber terrorism is added in **S.66 F** and **S. 67**, for publishing of obscene Information. **Sec. 67A** adds an offence of publishing material containing sexually explicit conduct and **Sec. 67B** for the offence of child pornography. Also the punishments for these cybercrimes were enhanced.

b) ***Significance of the term "Critical Information Infrastructure "*-Section 70** has a very important definition added by the IT (amendment) Act, 2008. The explanation to **Sec. 70** defines what is **"Critical information infrastructure".** It encompasses the computer resource the destruction of which not only has an adverse impact on defence of India but also economy, public health or safety. **Sections 70A** and **70B** envisaged the creation of particular agencies with clearly defined roles for implementing cyber security measures. While **section 70B** designated the existing **CERT-IN**, **section 70A** laid down the mandate for the creation of a new agency i.e **National Critical Information Infrastructure Protection Centre (NCIIPC)** through an official gazette notification issued by the Government of India to protect sectors designated as **CII**.

c) ***Composition of CAT*-**The amended Act has changed the composition of the **Cyber Appellate Tribunal** .The Presiding officer alone would earlier constitute the Cyber Regulations Appellate Tribunal which provision has now been amended. The tribunal would now consist of Chairperson and such number of members as Central Government may appoint. It is pertinent to note that there has not been any amendment in **Section 55** by 2008 amendments which states that no order of **CAT** shall be challenged on ground that there existed a defect in constitution of appellate tribunal.

d) ***The Corporate responsibility introduced in S. 43A*-**The corporate responsibility for data protection is incorporated in **S 43A** in the amended IT Act, 2000 whereby corporate bodies handling sensitive personal information or data in a computer resource are under an

obligation to ensure adoption of ***"reasonable security practices"*** to maintain its secrecy, failing which they may be liable to pay damages. Insertion of this provision is particular significance to **BPO** companies that handle such sensitive information in the regular course of their business. This provision is important to secure sensitive data and is hence a step in the right direction. The law explaining the definition of "reasonable security practices" is yet to be laid down and/or Central government is yet to frame its rules thereon.

3.2 ***Indian Computer Emergency Response Team (Cert-In)***[8] **-**

Cert-In is the most important constituent of India's cyber community. Till the specific and statutory role of government agencies was spelt out in **section 70 (A)** and **70 (B)** of the IT Act (Amended 2008), the bulk of the India's cyber-security concerns were the responsibility of one single agency: the **Computer Emergency Response Team – India (CERT-IN)**. By virtue of the above mentioned sections it has now been appointed as the National nodal agency for critical information infrastructure protection. Set up in 2004, it mapped India's cyber-security posture and was the sole point of contact for expertise on these matters to the government. It serves as the single point of contact for international cooperation with other CERTS. It's mandate states, 'ensure security of cyber space in the country by enhancing the security communications and information infrastructure, through proactive action and effective collaboration aimed at security incident prevention and response and security assurance'. A very important step is coordination between CERT and service providers, data centres, body corporate, and other persons (**Sec.70B (6)**). That will lead to effective performance of the role of CERT in. It has multiple roles education, alert system, emergency response, issuing guidelines, reporting of cyber incident amongst other functions. CERT-In, in collaboration with CII, **NASSCOM** and **Microsoft**, has created a portal **"secureyourpc.in"** to educate consumers on cyber security issues.[9]

3.2 NCIIPC[10]***-***

Although the IT Act was amended in 2008, the Gazette Notification that established the **National Critical Information Infrastructure Protection Centre (NCIIPC)** only came on 16 January 2014, almost six years later. NCIIPC's mission- *is to take all necessary measures to facilitate protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or destruction, through coherent coordination, synergy and raising information security awareness among all stakeholders and with a vision 'to facilitate safe, secure and resilient Information Infrastructure for Critical Sectors in the country.*

The sectors that have been designated as coming under NCIIPC's purview include defence; the banking and financial sector; ICT and telecommunication; transportation; power; energy; and the Ministries of Home Affairs, External Affairs, Heavy Industries and Niti Ayog (the erstwhile Planning Commission). Currently, NCIIPC follows a framework of conducting a **'vulnerability/threat/risk'** analysis (**V/T/R analysis**) for mapping the level of vulnerability of each designated sector during 'steady state operations', or the routine operations of an installation that follow a regular schedule [11]. Based on the V/T/R analysis, NCIIPC carries out a control configuration audit and brings in change management to mitigate any vulnerabilities.

3.3. National Cyber Security Policy (NCSP) 2013 [12]**-**

It was in 2013 that a national daily newspaper cited documents leaked by NSA whistleblower **Edward Snowden** that much of the **National Security Agency** surveillance was focused on India's

domestic politics and its strategic and commercial interests. This caused a furore amongst the people and the Government which unveiled a **National Cyber Security Policy, 2013** on July 2nd, 2013. It is a policy framework by **Department of Electronics and Information technology (DeitY**) and aims at protecting public & private infrastructure from cyber attacks. It also intends to safeguard critical information such as personal information, financial & banking information and sovereign data.

3.3.1.Major Highlights from the NCSP, 2013- Some of the key points of the National Cyber security Policy, 2013 are:

1. Set up of a 24×7 **National Critical Information Infrastructure Protection Centre (NCIIPC)** for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.
2. Creation of a task force consisting of 5,00,000 cyber security professionals in next five years through capacity building, skill development and training.
3. Provision for fiscal schemes and incentives to encourage entities to install, strengthen and upgrade information infrastructure with respect to cyber security.
4. Designation of CERT-In as the national nodal agency to coordinate cyber security related matters and have the local (state) CERT bodies to co-ordinate at the respective levels.
5. All organizations to designate a **CISO** and allot a security budget.
6. Use of **Open Standards for Cyber Security**.
7. Development of a dynamic legal framework to address cyber security challenges.
8. Encouragement of wider use of **Public Key Infrastructure (PKI)** for government services.
9. Engagement of infosec professionals / organizations to assist e-Governance initiatives, establish Centers of Excellence, cyber security concept labs for awareness and skill development through PPP – a common theme across all initiatives mentioned in this policy.
10. Apart from the common theme of PPP across the cyber security initiatives, the policy frequently mentions of developing an infrastructure for evaluating and certifying trustworthy ICT security products.

3.3.2. *Challenge[13] of Policy-*

The National Cyber Security Policy, 2013 takes holistic view of challenges and risks, and details out strategies for addressing them to a great extent even though it avoids going into specifics.

The challenge, however, is in implementation of the policy and defining the specifics.

Some of the concerns being raised are:

(1) *The declared cyber security policy has **proved to be a paper work** alone with no actual implementation till date.*

(2) *Indian cyber security policy has **failed to protect civil liberties** of Indians including privacy rights.*

(3) ***Civil liberties protection in cyberspace has been blatantly ignored** by Indian government surveillance projects have been kept intact*

(4) ***The offensive and defensive cyber security capabilities of India are still missing.***

(5) *India is considered to be a sitting duck in cyberspace and cyber security field and the proposed cyber security policy has failed to change this position.*

In light of these policy need to be revamped and it needs to be made dynamic to suit growing dynamicity of cyber space. Internet governance is an area where India can, and should, significantly improve its role, presence and influence given the fact it has a large community of internet users.

4. Conclusion:

We can think of the Internet as a parallel universe, a cyber-world as opposed to the real-world. In cyber-world people do much the same thing as in the real-world, such as chat, work, or go shopping. And, as in the real-world, there are dangers. In the real-world, we spend years as children learning about the world and all its dangers before we can safely go out on our own but same is not the case in cyber-world. People wander into cyber-world as cyber-toddlers or even cyber-infants. How can these people be expected to look after themselves in this strange new world? ... I believe that education must be the first step to computer security. Cyber-world is too complex and dangerous to jump into without understanding the dangers.

With the increasing proliferation of **Information and Communication Technologies (ICTs)** and the growing opportunity for real time borderless exchange, cyber security is a complex transnational issue that requires global cooperation for ensuring a safe Internet. In one of the **ECOSOC's** special events on **"Cyber security and Development"**, the **president of ECOSOC, H.E. Mr. Lazarous Kapambwe** in his concluding remarks pressed, [14]

"We have agreed that cyber security is a global issue that can only be solved through global partnership."

Just as drivers who share the road must also share responsibility for safety, we all now share the same global network, and thus must regard computer security as a necessary social responsibility. To me, anyone unwilling to take simple security precautions is a major, active part of the problem.

India is not yet a signatory to the ***BUDAPEST CONVENTION on CYBERCERIME***- which is the only international convention that we have on cyber crimes. India is still dealing with the question that whether she should sign the convention or not. But it has no doubt signed **bilateral agreement** [15] with **US** way back in **2000-01** establish a **Joint Working Group on Counter-Terrorism** and a **sub-group for cyber security** was also created. This was fist international initiative taken towards cyber security by India. India is nowadays actively taking part in the international conferences in this regard. Worldwide, actors at all levels, from individuals to nation states, need to ensure that cyberspace and the systems dependent on it are resilient to attack, in the face of constant growth in the scale and complexity of our networks, and enormous volumes of data and applications. Cyberspace and our assets within it need to be protected to ensure that critical digital infrastructures and services can operate effectively now and in the future. **"Cybercriminals aren't taking any time off, so why should we?"**

The faster you detect, the more attackers lose.

Reference

1. Cybersecurity and Human Rights in the age of Cyberveillance edited *by Joanna Kulesza, Roy Balleste;* p.4
2. Interrogation Report of Yasin Bhatkal. New Delhi, National Investigation Agency, 2014, p. 30.

3. PTI (2009). VoIP used by 26/11 planners. 150 test calls made before attack. *India Today*, 18 August,http://indiatoday.intoday.in/story/VOIP+used+by+2611+planners,+150+test+calls+made+before+attack/1/57314.html
4. CERT-IN Annual reports, available on the website, http://www.cert-in.org.in/
5. IT Act 2000 vs 2008- Implementation, Challenges, and the Role of Adjudicating Officers By Karnika Seth; *National Seminar on Enforcement of Cyberlaw , New Delhi on 8th May 2010; http://catindia.gov.in/writereaddata/ev_rvnrbv111912012.pdf*
6. Section 17 of the IT Act, 2000, appointed and defined the role of the CCA
7. IT Act 2000 vs 2008- Implementation, Challenges, and the Role of Adjudicating Officers By Karnika Seth; *National Seminar on Enforcement of Cyberlaw , New Delhi on 8th May 2010; **http://catindia.gov.in/writereaddata/ev_rvnrbv111912012.pdf***
8. IT Act 2000 vs 2008- Implementation, Challenges, and the Role of Adjudicating Officers By Karnika Seth; *National Seminar on Enforcement of Cyberlaw , New Delhi on 8th May 2010; **http://catindia.gov.in/writereaddata/ev_rvnrbv111912012.pdf***
9. XII five-year plan on information technology sector, Report of Sub-Group on Cyber Security, http://meity.gov.in/sites/upload_files/dit/files/Plan_Report_on_Cyber_Security.pdf
10. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity,%20IG%20%26%20IndianForeignPolicy_SDatta2016.pdf
11. Presentation on NCIIPC methodology by Director, NCIIPC at a CII workshop. Delhi, 4 November, 2014.
12. http://meity.gov.in/content/national-cyber-security-policy-2013
13. http://www.drishtiias.com/upscexamgsresourcesNATIONALCYBERSECURITYPOLICY2013
14. "(Cybersecurity: A global issue demanding a global approach | UN DESA | United Nations Department of Economic and Social Affairs, 9 dec. 2011 http://www.un.org/en/development/desa/news/ecosoc/cybersecuritydemandsglobalapproach.html
15. India-US Cybersecurity Forum: Fact Sheet. New Delhi, Ministry of External Affairs and Press Information Bureau, Government Of India,2 march, 2006, http://pib.nic.in/newsite/erelease.aspx?relid=16132.