CYBER SECURITY INITIATIVES BY THE INDIAN GOVERNMENT

Shobha Yadav
Research Scholar, MDU – CPAS, Gurugram (hr)
EMAIL- adv.shobhayadav@gmail.com

ABSTRACT

Due to covid 19 pandemic, cyber crime increasing very fast.An offender of cyber can easily hacked or destroyed any websites or portal or spreading viruses. Now, Cyberattack has become a major bane .Covid 19 is infected disease which caused coronavirus. As business, government agencies and human being are also rely on it. Today, we are living in this world where all work is done in a digital form. Its also affects our e-life. This pandemic has started a new trend for everyone to work from home. In this current e-age, crime is happened beyond the physical assault as well as mental torture. There is a need of cyber security for protection of data of the users and contains rising cyber crimes. From this research paper, researcher wants to highlights problem of Cyber security during covid 19 pandemic, government initiatives steps for the cyber security , range of cyber attack and cyber crime during coronavirus and lockdown measures to prevent the spread of the virus. Because misuse of digital technology for the criminal activities is increasing day to day which is result of cyber crime .

Keywords : Cyber crime, Covid 19, Information technology, Cyber security, Coronovirus

INTRODUCTION

Cyber crimes in India caused Rs 1.25 trillion loss in 2019. Cyber threats will continue to increase as the country starts developing smart cities and rolling out 5G network, among other initiatives. There are only a few Indian companies who are making some of the cyber security products and there is a big vacuum in the sector. So, a dedicated industry forum for cyber security should be set up to develop trusted indigenous solutions to check cyber attacks.The quantity of digital protection episodes has bit by bit expanded in India in the course of the most recent couple of years. These episodes incorporate phishing, site interruptions and ruinations, infection and forswearing of administration assaults among others. Albeit, the public authority has taken certain network protection drives as talked about underneath, more sweeping and forceful measures are needed to address the rising difficulties. Cyber attacks have been occurring with increasing frequency. For example, leak of personal information of 3.2 million debit cards in 2016 and the Data Theft AtZomato (2017), Wannacry Ransomware (2017), PETYA Ransomware (2017) etc.

Further, Cyber security has become an integral aspect of national security. Moreover, its area of influence extends far beyond military domains to cover all aspects of a nation's governance, economy and welfare.Although India was one of the few countries to launch a cybersecurity policy in 2013, not much has transpired in terms of a coordinated cyber approach. Thus, there is a need for a comprehensive cyber security policy in India.

CYBER : The term, 'Cyber' is used in relation to the culture of computers, information technology, and virtual reality. The connection between internet ecosystems forms cyberspace. The threat to cyberspace leads to an issue and gives rise to the need for cybersecurity

Cyber security is protecting the internet including basic data foundation from attacks, damage, abuse or misuse and monetary undercover work.

Cyber space : A worldwide area inside the data climate comprising of the associated organization of data innovation frameworks, including the Web, media communications organizations, PC frameworks, and installed processors and regulators.

Digital Attack: It's anything but a malignant and purposeful attemped by an individual or association to breach the data system of another individual or association / organization.

Critical Information Infrastructure: According to Section 70(1) of the Information Technology Act, 2000 CII defined as a "computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety".

The **National Security Council** (NSC) of India is a three-tiered organization that **oversees political, economic, energy and security issues of strategic concern.**

MOTIVES BEHIND THE CYBER ATTACKS

- To attack basic assets of a country.
- To look for business acquire by hacking banks and monetary foundations
- To infiltrate into both corporate and military information workers to acquire plans and insight.
- To hack websites to virally convey a directive for some particular mission identified

with governmental issues and society.

TYPES OF CYBER ATTACKS

- **Phishing:** It is the method of trying to gather personal data using deceptive e-mails and websites.
- **Denial of Service attacks:** A Denial-of-Service (DoS) attack is an attack meant to closed down a machine or network, making it unavailable to its expected users. DoS attacks accomplish this by flooding the objective with traffic, or sending it data that triggers an accident.
- **Man-in-the-middle (MitM) attacks,** also known as eavesdropping or snooping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interfere with the traffic, they can filter and steal data.
- **Malware,** short for malignant programming refers to any sort of programming that is intended to make harm a solitary PC, worker, or PC organization. Ransomware, Spyware, Worms, viruses, and Trojans are generally varities of malware**.**
- **Social engineering** is an attack that depends on human association to trick users into breaking security strategies in order to gain sensitive data that is ordinarily protected

COMPONENTS OF CYBER SECURITY

- **Application Security:** It includes measures or counter-measures that are taken during an application's advent process to protect it from the danger that can come through defects in the app plan, improvement, deployment, upgrade or maintenance.
- **Data security:** It is related to the protection of data from an unapproved access to avoid identity theft and to protect privacy or ensure the protection.
- **Network Security:** It includes activities to protect the convenience,dependability, uprightness and safety of the network.
- **Disaster Recovery Planning:** It is a process that includes performing risk evaluation, building up needs, creating recuperation techniques if there should be an occurrence of an assault.

NEED OF THE CYBER SECURITY

There were **6.97 lakh** cyber security incidents reported in the **first eight months of 2020,** nearly equivalent to the previous four years combined, according to information reported to and tracked by Indian Computer Emergency Response Team (CERT-in).

Increased Digital usage Post-Covid: Critical infrastructure is getting digitised in a very fast way — this includes **financial services, banks, power, manufacturing, nuclear power plants etc.**

- **For Individuals:** Images, videos and other personal data which is shared by any person on social networking sites can be inappropriately used by others, leading to genuine and surprisingly hazardous incidents.
- **For Business Organizations:** Companies have a lot of data and information on their computer systems. A cyber attack may lead to loss of competitive data (such as patents or original work), loss of employees/customers or clients private data resulting into complete loss of public trust on honesty of the association
- **For Government:** A local, state or central government maintains huge amount of private information related to country (geographical, military strategic assets etc.) and citizens. Unauthorized access to the data can lead to serious threats on a country.
- **National Security Imperative:** The change in military doctrines favouring the need to raise cyber commands reflects a shift in strategies, which include building deterrence in cyberspace. The need for a competent cyber security infrastructure as part of national security was first emphasized by the Kargil Review Committee 1999.
- **Increasing Importance of Digital Economy:** The digital economy today comprises 14-15% of India's total economy, and is targeted to reach 20% by 2024.
- **Added Complexity:** With more inclusion of artificial intelligence (AI), machine learning (ML), data analytics, cloud computing and Internet of Things (IoT), cyberspace will become a complex domain, giving rise to issues of a techno-legal nature.
- **Securing Data:** Data is referred to as the currency of the 21st century and due to its bulk creation owing to India's population, several international companies (Google, Amazon etc.) are trying to have access to it. It Given this there are issues related to data sovereignty, data localisation, internet governance, etc. Thus, there is a need to build strong cyber security architecture.

INITIATIVES STEPS TAKEN BY THE GOVT.

The government of India is taking many initiatives to enhance cybersecurity. With the rapid development of information technology, it is critical to provide a safe and secure cyberspace. For the attempt of creating a 'cyber-secure nation' for businesses and individuals, the government of India is reportedly set to unveil its cybersecurity strategy policy in January 2020 to achieve the target of a $5 trillion economy. Government of India working closly to deal with cyber security issues, many initiatives like CERT-In, NCIIPC, website and application audits, crisis management plan, regular training and PDP bill etc are in place and ready to tackle any security issues.

⇨ **National Critical Information Infrastructure Protection Centre (NCIIPC).**National Computer Emergency Response Team (CERT-in) functions as the nodal agency for coordination of all cyber security efforts, emergency responses, and crisis management.Protection and resilience of critical information infrastructure with the **National Critical Information Infrastructure Protection Centre** (NCIIPC) operating as the nodal agency. NCIIPC has been created under Information Technology Act, 2000 to secure India's critical information infrastructure. It is based in New Delhi. NCIIPC is a central government establishment, formed to protect critical information of our country, which has an enormous impact on national security, economic growth, or public healthcare. This was amended as per the provisions of section 70A of the Information Technology (IT) Act, 2000.

⇨ **Information Technology Act, 2000.**The act regulates use of computers, computer systems, computer networks and also data and information in electronic format.The act lists down among other things, following as offences:

- Tampering with computer source documents.
- Hacking with computer system
- Act of cyber terrorism i.e. accessing a protected system with the intention of threatening the unity, integrity, sovereignty or security of country.
- Cheating using computer resource etc.

⇨ **National Cyber Policy, 2013.** The Government of India took the first formalized step towards cyber security in 2013, vide the Ministry of Communication and Information Technology, Department of

Electronics and Information Technology's National Cyber Security Policy, 2013.The Policy is aimed at building a secure and resilient cyberspace for citizens, businesses and the Government. Its mission is to protect cyberspace information and infrastructure, build capabilities to prevent and respond to cyber attacks, and minimise damages through coordinated efforts of institutional structures, people, processes, and technology.

⇨ **Indian Cyber Crime Coordination Centre (I4C):** The I4C will assist in centralising cyber security investigations, prioritise the development of response tools and bring together private companies to contain the menace.

⇨ **The Personal Data Protection Bill 19**to secure citizens data. the approval of Personal Data Protection (PDP) Bill by the union government in order to protect Indian users from global breaches, which focuses on data localisation. The bill implies the storage and processing of any critical information related to individuals only in India. The **Personal Data Protection Bill** draft 2019 proposes to store personal data within India only, it can not possess abroad without approval of **Data Protection Agency**, critical data can not go abroad. It proposes heavy penalties for any violation, INR 5 crores for a minor violation and INR 15 crores for serious violation and organization executives can also face a jail term.

⇨ **Indian Computer Emergency Response Team (CERT-IN):** It is an organisation of the Ministry of Electronics and Information Technology, Government of India, with the objective of securing Indian cyberspace. It is the nodal agency which deals with cybersecurity threats like hacking and phishing. The implementation of anti-phishing and cybersecurity awareness training across India's government agencies has assisted government employees in fighting against cybercrimes.

⇨ **Online Cyber Crime Reporting Portal** : It Launched in 2019, it is a citizen-centric initiative enabling citizens to report cybercrimes online.The portal specifically focuses on crimes against women, children, particularly child pornography, child sex abuse material, online content pertaining to rapes/gang rapes, etc. It also focuses on crimes like financial crime and social media related crimes like stalking, cyberbullying, etc.It will improve the capacity of law enforcement agencies to investigate the cases after successful completion by improving coordination amongst the law enforcement agencies of different States, districts and police stations.

- ⇨ **Cyber Surakshit Bharat Initiative**: It was dispatched in 2018 with a mean to spread awareness about cybercrime and building limit with respect to wellbeing measures for Chief Information Security Officials (CISOs) and bleeding edge IT staff across all administration offices.
- ⇨ **National Cyber Security Coordination Centre (N**CCC): In 2017, the NCCC was created. Its order is to filter web traffic and correspondence metadata (which are little bits of data covered up inside every correspondence) coming into the nation to identify real time cyber threats.
- ⇨ **Cyber Swachhta Kendra**: In 2017, this stage was originated for web clients with clean their PCs and gadgets by clearing out viruses and malware. The "Cyber Swachhta Kendra" (Botnet Cleaning and Malware Analysis Centre) is a part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology . To combat cyber security violations and prevent their increase, Government of India's Computer Emergency Response Team (CERT-in) in February 2017 launched 'Cyber Swachhta Kendra' (Botnet Cleaning and Malware Analysis Centre) a new desktop and mobile security solution for cyber security in India.

The centre is operated by CERT-in under Section 70B of the Information Technology Act, 2000. The solution, which is a part of the Ministry of Electronics and Information Technology's Digital India initiative, will detect botnet infections in India and prevent further infections by notifying, enable cleaning and securing systems of end-users.

- ⇨ Training of 1.14 Lakh persons through 52 institutions under the **Information Security Education and Awareness Project (ISEA)** – a project to raise awareness and to provide research, education and training in the field of Information Security.

- ⇨ **International cooperation:** Looking forward into protected cyber ecosystem, India has joined hands with few created nations like the United States, Singapore, Japan, etc. These agreements will assist India to challenge even more sophisticated cyber threats.

CONCLUSION AND SUGGESTIONS

India is the second-fastest digital adapter among 17 of the most-digital economies globally, and rapid digitisation does require forward-looking measures to boost cybersecurity.There is a lack of cyber security workforce and lack of cyber active defence. India is mostly depend on foreign players for cyber security tool . there is a lacks indigenisation in hardware as well as software cybersecurity tools.This makes India's cyberspace vulnerable to cyberattacks motivated by state and non-state actors. social media is becoming a powerful tool for dissemination of “information” making it difficult to differentiate fact from fake news.

- **There should be need of creating awareness .**National cybersecurity projects such as the National Cyber Coordination Centre (NCCC), National Critical Information Infrastructure Protection Centre (NCIIPC) and the Computer Emergency Response Team (CERT) need to be strengthened manifold and reviewed. There is a need for an apex body to ensure operational coordination amongst various agencies and ministries.
- Cyber deterrence can be envisaged on the lines of strategic deterrence to dissuade cyberattackers. We need to acquire offensive capabilities for effective deterrence in cyberspace
- **Bringing Cyber Security in Education:** Educational institutions including central universities, private universities, industry associations, Industrial Training Institutes (ITIs) must incorporate courses on cybersecurity.There is a need to create opportunities for developing software to safeguard cyber security and digital communications.
  - o The Government of India may consider including cybersecurity architecture in its MAKE IN INDIA PROGRAMME.
  - o Also, there is a need to create suitable hardware on a unique Indian pattern that can serve localised needs.
- Given the future of technology under Industrial Revolution 4.0, India requires a

strong cybersecurity framework based on the 4D principles i.e. Deter, Detect, Destroy and Document so that it can subverse all attempts towards any cyber challenges.Increased awareness about cyber threats for which digital literacy is required first.

- India needs to secure its computing environment and IoT with current tools, patches, updates and best known methods in a timely manner.
- The need of the hour for Indian government is to develop core skills in cyber security, data integrity and data security fields while also setting stringent cyber security standards to protect banks and financial institutions.

REFERENCES

- Government of India launches 'Cyber Swachhta Kendra'; a new mobile and desktop security solution, Tech 2, February 21, 2017, http://tech.firstpost.com/news-analysis/government-of-india-launches-cyber-swachhta-kendra-a-new-mobile-and-desktop-security-solution-363415.html
- As India Gears Up for Cybersecurity Challenges, Threats Are Multiplying, Security Intelligence, August 2016, https://securityintelligence.com/as-india-gears-up-for-cybersecurity-challenges-threats-are-multiplying/
- National Cyber Security Policy, 2013, http://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf
- IT Minister orders measures to strengthen India's cyber security, The Economic Times, 13 December 2016, http://economictimes.indiatimes.com/articleshow/55963728.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- http://www.cyberswachhtakendra.gov.in/about.htmL
- Government of India launches 'Cyber Swachhta Kendra'; a new mobile and desktop security solution, Tech 2, February 21, 2017,
- http://tech.firstpost.com/news-analysis/government-of-india-launches-cyber-swachhta-kendra-a-new-mobile-and-desktop-security-solution-363415.html
- Cisco India unveils three cyber security initiatives, The Week, 22 December 2016,

- http://www.theweek.in/news/sci-tech/cisco-india-unveils-three-cyber-security-initiatives.html
- DSCI. (2013). Analysis of National Cyber Security Policy (NCSP–2013). New Delhi: Data Security Council of India.
- Gercke. (2009). Understanding Cybercrime: A Guide for Developing Countries, Geneva: ITU publication.
- FACT SHEET: Framework for the U.S.-India Cyber Relationship, The White House, Office of the Press Secretary,
- Government of India. (2011). Discussion Draft on National Cyber Security Policy. New Delhi: DIETY.
- Government of India. (2012). "National Telecom Policy (NTP) – 2012." Ministry of Communication and Information Technology (NTP). New Delhi, June 13. http://www.dot.gov.in/sites/default/files/NTP-06.06.2012-final_0.pdf.
- Government of India. (2012). National Cyber Security Strategy, India: DEITY.
- IANS. (2014). "69 Percent of Cyberattacks Targeted at Large Companies in India: Report." Business Standard, New Delhi, April 24
- Kaushik, R. K. (2014). "Cyber Security Needs Urgent Attention of Indian Government." http://cybersecurityforindia.blogspot.in/2014/09/cyber-security-needs-urgent-attention.html.
- https://obamawhitehouse.archives.gov/the-press-office/2016/06/07/fact-sheet-framework-us-india-cyber-relationship
- Upgrading India's cyber security architecture, The Hindu, 9 March 2016, http://www.thehindu.com/opinion/columns/upgrading-indias-cyber-security-architecture/article8327987.ece
- India's Cyber Protection body pushes Ahead, Hindustan Times. 29 January 2014
- http://www.hindustantimes.com/india/india-s-cyber-protection-body-pushes-ahead/story-4xa9tjaz6ycfDpVg95YqPL.html