SAVING THE WORLD FROM BLOODLESS WAR: CYBERSECURITY

Saumya Singh

University institute of legal studies, Punjab University

Cybersecurity is a broad phrase referring to the prevention of unauthorised and malafide access to any digital device like computers, laptops, mobiles or any network system. Cybersecurity is a nexus issuance that cuts across multifarious factors and there is a dire need for multidimensional initiative and acknowledgement, which has proven to be confrontational for governments globally. As in the recent past, the globe has suffered periodically with ransomware attacks like Wannacry Malware, Blackrock Malware, Agent Smith, Operation Aurora, PETYA Global and the chain goes on.[1]

The ASSOCHAM Organisation studies have shown that there is a 457% increase in cyber-attacks in the last five years.[2] Accompanying ASSOCHAM data, new statistics of financial stability report by RBI revealed that attacks on the banking system have been increased by twice its rate in last years.[3]

The history dawning to the cyber-attack is not too long ago. It all started in 1969 when a professor from University of California was working on a project where he sent the message 'log in' to a standard research institute; but while working on the text, his system crashed and faced the first cyber-attack in the world of digitalisation. In 1971, Bob Thomas created his first virus called CREEPER and it took two years to design an anti-virus to fight against it.[4] These recurrent incidents derived world forces to construct cybersecurity as a reality.

Cybersecurity is propagating its roots all over the world. Prominent effects have been seen in India in the form of massive spending over fast digitation movement.[5] Leading global security solution companies say that the revenue growth in India has accelerated and today, security is

---

[1] HT Tech, *Blackrock to Agent Smith*, HT, (20 July2020, 8:06AM) https://tech.hindustantimes.com/amp/tech/news/blackrock-to-agent-smith-5--71595181807391.html#aoh=16069753417186&referrer=https://www.google.com&csi=0

[2] ASSOCHAM Office, *India saw475% rise in cybercrime in five year*, ASSOCHAM, (February 21, 2018) https://www.assocham.org/newsdetail.php?id=6755

[3] RBI Report, *Around 50,000 Cyber Frauds in India during 2018-19:RBI*, CISOMAG, (July14 2019) https://cisomag.eccouncil.org/around-50000-cyberfruad-report-in-india-during-2018-19-rbi/

[4] Steven Brocklehurst , *The man who discovered the first virus*, KASPERSKY, (24 July 2016), https://www.kaspersky.co.in/resource-center/threats/a-brrief-history-of-the-future-holds

[5] *Id* at.4

a major discussion point at the topmost level in customer companies. Hence, we have to fathom each aspect of cyber threat in detail. Few of them are as follows:

- Cyber Threat can be explained as an offence that is committed against individuals or groups with a mala fide intention to harm the reputation of the victim or cause physical or mental harm, using modern telecommunication networks.
- Cyber Terrorism is the use of the internet to conduct violent acts that result in a loss of life or cause significant bodily harm. The objective of such an attack can be to promote a political or ideological agenda. Recent activities of ISIS in the Middle East and a series of videos released by them are potential cyber terrors. They use Cyberspace to sway vulnerable people to join ISIS.[6]
- Cyber Espionage is the act of obtaining secrets and information without the consent and authorisation of the holder with proxy servers, cracking techniques and malicious software to promote a political agenda or social change. The Chinese Crackers saw the espionage attack in 2009 in PMO of India computers.[7]
- Cyber Stalking is a term referred to the use of the internet, e-mail, or other electronic communication devices to stalk people.
- Dissemination of Malicious Software (Malware) is a software designed to perform illegal acts via the computer network. Ransomware is the most appropriate example as this software is designed to access a computer system, typically by encryption.[8]

Vulnerabilities of Cyber Spacing

However, these threats can be minimised through cybersecurity policies and software, but cyberspace has inherent vulnerabilities that cannot be removed.

- Innumerable entry points- while connected to the internet, as every device is connected to each other subsequently, every device becomes an entry point into the system and any of them can be the target of a cyber-attack. In a nutshell, each device connected to the internet is at potential risk for an attack.

[6] NTI Bench, *Addressing potentially catastrophic of cyber terrorism*, (20 July2020 ,02:45 AM), https://www.nti.org/about/cyber/
[7] Express news Service, *Chinese hacked PMO computers, says Narayan* , THE INDIAN EXPRESS, (Jan 19 2010, 8:18). , https://archive.indianexpress.com/news/chinese-computer-says-narayan/569075/
[8] Id .at 1

- Assigning attribution– Internet technology makes it easy to debauch attribution to other parties. It can be easily explained by saying that a real criminal can misguide the investigation process by attributing his criminal charges to a false party.
- Capable of waging attacks- In cyber warfare, hackers can potentially control nuclear or defence facilities in enemy nations by finding a back door in their computer network.
- Advanced Precision Threats (APTs) carried out by anonymous hackers are often silent and go unperceived for a long period of time. We lack the technology to detect the APTs' silent attack in time.

India and Cyber Security

Indian Government in the last few years has seen robust growth in the Internet users' base with over 550 million users, making India the second-largest internet consumer.[9] The unexceptional growth of the cyber world brings unwanted guests as cyber threats. According to a research conducted by Pricewaterhouse Cooper (PwC), India's cybersecurity market is expected to grow massively from $1.97 billion in 2019 to $3.05 billion by 2022, giving an annual growth rate of 15.6% approx., which is half time the global rate.[10] Although India is one of the few countries to launch a cybersecurity policy in 2013, not much has transpired in terms of coordination cyber approach. Thus, there is a need for a compendious cybersecurity policy in India.

Need for a Cyber Security Framework

Being a developing advanced cyberspace network, India remains the fifth most vulnerable country in the world in terms of cybersecurity breaches, according to the Internal Security Threat Report of 2017 by Symantec.[11] Hence, this shows us the loopholes of India cyber spacing and branches out many concerns like:

- Over Regulatory Bodies - Unlike the US, Singapore, the U.K where there is a single umbrella organisation dealing in cybersecurity. India has several central bodies that deal with cyber issues and each has a separate reporting structure, with this each state

[9] Sunil Gupta, *India may have 800 million internet users by 2023,* FE, (Jan 8, 2020) ,page 12 https://www.financialexpress.com/industry/technology/india-may-have-800-million-internet-users-by-2023-if-it-can-get-this-factor-right/1816771/

[10] PWC Office, *Cyber security and India*,PWC (23 May 2019 , 04;50 PM), https://www.pwc.in /cyber-security.html

[11] *Internet Security Threat Report,* Symantec, (March 2018), https://docs,broadcom./doc/istr-23-executive-summary-en

government has its own Cyber emergency Response Team making the whole system quite haphazard and multiple control authorities make working difficult to regulate.[12]

- Lack of Cybersecurity workforce- Indian workforce for the IT sector is considerably less than its requirement. As seeing the Indian perception for government jobs, there are quite less opportunities for IT students in the government sector. Moreover, there is a growing demand for professionals in AI (artificial intelligence), Block chain Technology, Internet of Things and Machine Learning and according to several estimates; there is a need for at least 3 million cybersecurity professionals today.[13]
- The disparity in the use of devices for internet access- India's market share of expensive and highly security norm phones is only 1% mobile users.[14] This vast gap between the security offered by expensive phones and lower-cost mobile makes it impossible for legal and technical standards to be set for data protection by regulators.
- Lack of Awareness – One of the main weaknesses in preventive measures has been the lack of awareness about cybersecurity among the users. In India, there is no national regulatory policy for cybersecurity that leads to a lack of awareness at both company and individual level. Even experts say that lack of knowledge among people about cybercrimes makes them act negligent of their personal data and this makes a fraudster's job easy.[15]

These factors pose serious concerns for the growing space of digitalisation in India. Hence, many steps have been taken by government legislation to deal with cyber threats at the centre and state level. Let us get an overview of these regulatory steps taken by the government.

Legislative Measures

- Information Technology Act, 2000- It is the primary law established to deal with cybercrime and digital commerce in India. The Act has adopted a digital approach in which paper-based requirements such as document, record and signature are

---

[12] *Id.* at 9

[13] Et Bureau, *India techies rescues: Country wants to recruit IT professionals*, (March 09, 2018 ,11:38AM IST), TET, https://m.economictimes.com/nri/visa-and-immigration/ -indian-it-professionals/amp_articleshow/63220607.cms#aoh=16069790502520&referrer=https://www.google.com&csi=0

[14] Abhik Sengupta , *Apple won't make flagship iPhone models in India*, (3 March 2020, 14:28 IST), NDTV, ps://gadgets.ndtv.com/mobiles/news/iphone-11-production-not-coming-to-india- 2189060?amp=1&akamai-rum=off#aoh=16069793524323&referrer=https%3A%2F%2Fwww.google.com&amp_tf=From%20%251%24s

[15] PWC Office, *Cyber security and India*,PWC, (23 May 2019) , 04;50 pm, https://www.pwc.in/consulting/cyber-security.html

replaced with their electronic counterparts. The IT act has been amended in 2008[16]. Now, important sections which deal with the today is growing threat are – section 43 (data protection), section 66 (Hacking), section 66A (measures against sending offensive messages), section 66B (punishment for illegal possessing stolen compute resource), section 69 (cybercrime), section 72 (privacy and confidentiality) among others.[17]

- National Cyber Security Policy, 2013 is a policy framework by the Department of Electronic and Information Technology. It aims at protecting the public and private infrastructure from cyber-attack. The policy also intends to safeguard information such as personal information and sovereign data".

Institutional Measures

- National Technical Research Organisation is a technical intelligence Agency under National Security Advisory in the Prime Minister's Office. It is the main agency designed to protect and handle national, critical, infrastructural and all other cybersecurity incidents in critical sectors of the country.
- National Critical Information Infrastructure Protection Centre (NCIIPC) has been made to battle cyber threats in strategic areas such as air control, nuclear and space. It will function under the National Research Organisation, a technical intelligence-gathering agency.
- National cyber coordination centre- The union Minister of Electronics and Information Technology has announced NCCC will be scanning the country's web traffic to detect cybersecurity and e–surveillance agencies. It will be India's first layer of cyber threat monitoring and all communication and government and private service providers will be monitored round the clock.

Stress on the development of technology in the field of cybersecurity with the capacity of skilled human resources can make India cyberspace robust. The priority of cybersecurity should be no longer optional but one of the pillars of India's internal-external securities. The innovation and concerns regarding cyber threat should be discussed globally so that each side

[16] Ministry of Electronic & Information Technology Report, IT Act ,2008 (Amendment) https://www.meity.gov.in/content/information-technology-act
[17] *Id.* at 15

of the coin is being evaluated closely and there is no edge of failed services. Therefore, international policymakers and peacekeepers take numerous steps.

International Measures:

- Global Conference on Cyber Space is one of the world's largest conferences in the field of cyberspace, which is being hosted by India for the first time in its 5th edition where international leaders, policymakers, industry experts, think tank and cyber experts will gather to deliberate on issues and challenges for optimally using cyberspace.
- The Global Centre for Cybersecurity is launched by the World Economic Forum to serve as a laboratory and early-warning think tank for future cybersecurity scenarios and help in building secure global cyberspace.
- Budapest Convention on cybercrime is the first global treaty seeking to address internet and cybercrime by harmonising national law, improving investigative techniques and increasing cooperation among nations. The convention has 56 members including the US and the U.K.[18]

Conclusion:

Cybersecurity is needed in the present era of increasing connectivity. Though the Government is taking many steps to enhance the world of networking for us, we too have a corporeal duty for the safety and security of our country so that we do not lack in any place. Today's government has an urgent need for the advancement of R&D to develop innovative technologies to fight increasing cybersecurity issues. With this immediate attention has to be given to human workforce to increase the number of pundits who can efficaciously manage the cybersecurity of the country and as responsible citizens, we have to develop awareness towards the cyber world by taking part in campaigns and workshops and guide the people about the importance of cybersecurity in the 21st century.

[18] Convention on Cybercrime, 23 November 2001,https://www.coe.int/en/web/cybercrime/the-budapest-convention