www.revistageintec.net
ISSN: 2237-0722
revista GEINTEC
Gestão, Inovação e Tecnologias

Competence in Cybercrime: A Review of Existing Laws

Nibras Salim Khudhair[1]
[1]Law Department - Al Kunooze University College, Basra, Iraq.
[1]nibras.s@kunoozu.edu.iq

Abstract

Transformational cyber security and training programmes are urgently required to produce individuals and workforce capable of addressing company risks posed by existing and emerging cyber threats. This paper presents a cyber security model of India and give an analytical approach to the competence with the crime, a continuous hierarchy of learning. The chapter combines the cyber-security domain, academic development, and the pyramid of learning continuum, as well as cyber-security standards from state, to create a model of cyber-security skills appropriate for people's education and the broader workforce. This fundamental approach to building cyber skills and training programmes results in trained individuals and workers who can reduce cyber hazards in the business environment throughout the globe. In popular culture, such experts are sometimes depicted as lone hackers. Cybersecurity specialists, on the other hand, must communicate with a variety of people all of the time. They must also have a high level of personal integrity. The practise of cyber hunting is a different approach to traditional cyber security, in which technologies and human intelligence are used to discover potential threats. Using firewall, antivirus, and intrusion detection software, this strategy seeks to detect penetration and prevent hacker penetration.

Key-words: Personal Integrity, Detect Penetration, Criminal Intruders.

1. Introduction

Because of our increasing reliance on the Internet, cyber security has become a global issue. The economic and national security issues facing states, established and emerging countries, and also public and private corporations, are among the most important concerns that governments, business, and all other organisations face. Both cash forces and cyber-attacks may now actually occur beyond geographic borders due to the Internet, which makes companies from both domestic and foreign sectors vulnerable.[1]Threats to the internet come from a variety of places, including governments, many terrorist organisations, employees, and criminal intruders. Assaults on essential wings, such as derailment of trains, pollution of water bodies,[2] and technical alteration in the electrical power grid system, can occur from theft of staff's personal details to assaults on essential infrastructure.[3]Due to the tremendous cost of cybercrime to society, administration, and citizens, dealing with it has become critical. Consider the financial damage incurred as a result of cyberattacks. It is estimated that commercial organisations spend $240,000 each day, and that shops spend more than $100,000 each hour.

Cybersecurity has risen to the top of the political agenda in the United States Presidential Proclamation of 2016.[4] It is a vital responsibility of institutions and individuals that necessitates effective collaboration between these institutions and the community, along with individuals and the wider working people.[5] According to Russel[6], the general population is becoming more aware of cyber threats. However, evidence suggests that cybercrime has increased significantly during the previous few years. For example, cybercrime has risen from fourth to second position in terms of global economic crime.[7]As a result, continuing cyber security education must be modified as soon as possible in order to produce individuals and employees capable of addressing enterprise risks posed by current and future cyber threats. Such modifications and changes to current cybersecurity norms are necessary due to the many facets of cybersecurity, the scope of cyber assaults and activity, and the goals of cyber assaults.

2. Background

According to a cybersecurity software company's study, Norton Lifelock, more than 59 percent of Indians have been victims of cyber-crime in the last year. In ten countries—India, the United States Germany, Italy, France, Japan, New Zealand, the Netherlands, the United Kingdom, and Australia—more than 10,000 people were questioned (US). These Indian adults numbered in the

[1] Patel, Durgambini A., and Sanjana Bharadwaj. 2020. "The Code on Social Security in India, 2019."

[2] Yang, Bo, Hongxin Hu, and Yunyun Xie. 2020. "A Review on Cyber Security of Digital Electro-Hydraulic Control System of Steam Turbine." In 2020 IEEE 4th Conference on Energy Internet and Energy System Integration (EI2).

[3] Sahoo, Subham, Tomislav Dragicevic, and Frede Blaabjerg. 2020. "Cyber Security in Control of Grid-Tied Power Electronic Converters–Challenges and Vulnerabilities." IEEE Journal of Emerging and Selected Topics in Power Electronics, 1–15.

[4] US Presidential Proclamation 9508, 2016.

[5] Ch, Rupa, Thippa Reddy Gadekallu, Mustufa Haider Abidi, and Abdulrahman Al-Ahmari. 2020. "Computational System to Classify Cyber Crime Offenses Using Machine Learning." Sustainability 12 (10): 4087.

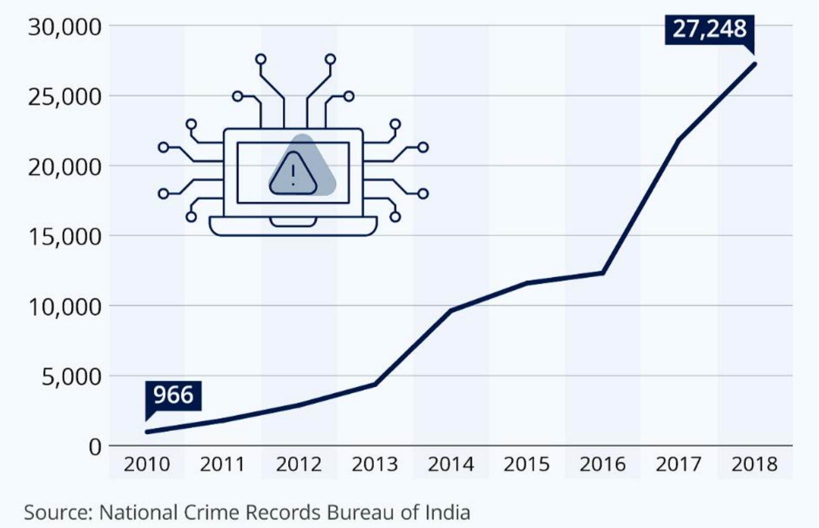
[6] Russell (2017)

[7] according to the Global Economic Crime Survey

thousands. According to the report, 27 m Indian adults have suffered identity theft in the previous 12 months, and 52% of the country's adults are unaware of how to protect themselves against cybercrime. In a year of restrictions and constraints, cyber criminals have not been discarded[8]. In the previous year, more Indians have had their identities stolen, with the majority of them being thoughtful about their privacy, Mr Ritesh Chopra, sales and field marketing manager for India in MNC Norton LifeLock's as well as SAARC countries, stated as much.[9]

Cyber security-related mishaps have increased in the recent year, mainly to the rising use of remote working technology. In India, there has been no growth in cybercrime. A national poll in the United States found that at least a quarter of surveyed Americans detected unauthorised access to an account or to an appliance in the previous one year.[10] An estimated 719 million hours of American cyber crime time was spent over 6.7 hours seeking to resolve challenges that arose over the preceding 12 months out of the approximately 108 million Americans (41 percent).

Figure 1 - Increase in cybercrime in India between 2010-2018 (Image credit: Satista website)



Source: National Crime Records Bureau of India

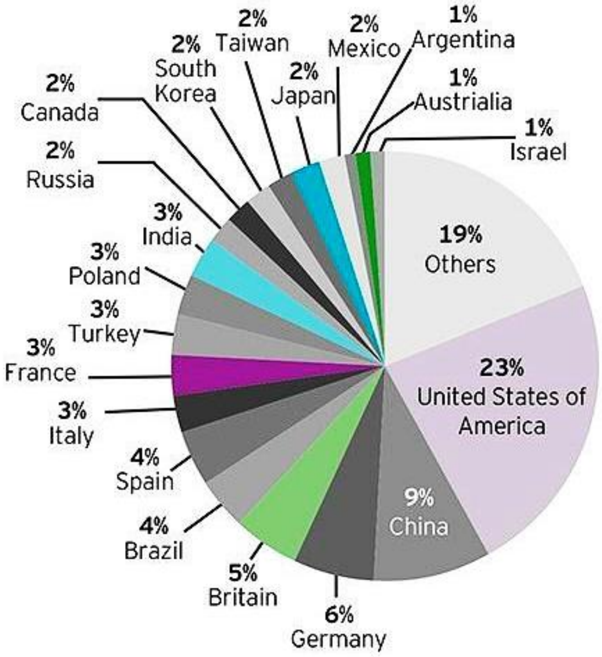
Consumers in India lost more than US$18 billion in 2017 as a result of cyber theft, according to estimates. These forecasts, on the other hand, were made solely on the basis of the data provided. Due to less awareness of cyber crime & the procedures used to categorise it in a country like India, the true figures may be significantly underreported. Some latest government efforts, like a dedicated

[8] https://www.google.com/amp/s/www.thehindu.com/sci-tech/technology/317-lakhs-cybercrimes-in-india-in-just-18-months-says-govt/article34027225.ece/amp/
[9] Vijai, C. 2020. "Cloud-Based E-Governance in India." Social Science Research Network.
[10]Norton Poll

online portal for reporting cybercrime from 2017 onwards, might be a key contributor to the increase of reporting in cybercrimes and their resolutions.[11]

Remote work infrastructure, on the other hand, is simply one method for hackers to get access to businesses. Many hackers have attempted to take advantage of the virus to put users' devices and accounts at risk. Phishing is one of them, since it pretends to inform customers about vaccines or other measures related to the preservation of human life. Checkpoint Security, a security firm, has recorded about 192,000 such attacks every week as of May 12, 2020.[12]

Figure 2 - Top 20 countries affected by cybercrimes



According to NCRB data, there were nearly 45,000 cybercrime incidents reported in the year 2019 alone, compared to only about 29,000 in 2018. With nearly 12,000 cybercrime incidents reported in just one year, Karnataka topped the chart as the state with highest cybercrime. Karnataka was closely followed by the most populous states, Uttar Pradesh, with close to 11,500 incidents reported under section 66 of the IT Act. These two states were followed by Maharashtra (close to 5000 cybercrime incidents) and Telangana and Assam, with over 2500 incidents of cybercrime

[11] The Hindu, (Date of Publication) "317 Lakhs Crybercrimes in Indian in just 18 months." Retrieved from www.thehindu.com/sci-tech/technology/317-lakhs-cybercrimes-in-india-in-just-18-months-says-govt/article34027225.ece/amp/ (Last accessed 31 May 2021).

[12] Howling, Matt. 2020. "Staying Safe from Cyber-Crime and Scams."

reported in each state. Among Union Territories, the National Capital of Delhi alone accounted for close to four in every five reported cybercrime incidents.[13][14]

As per the data gathered, nearly 3,17,500 cyber-crime occurrences, approx. 5,800 cyber-crime events, 50,805 cyber-crime events, and 535 FIRs have happened in the state of Karnataka from the program's inception till February 28, 2021.According to the Federal Investigative Office's (FIO) US Internet Crime Complaint Centre (IC3) Internet Crime Report 2019, India is the world's third most susceptible country to Internet crimes. Apart from the United States, the UK is the leading victim of Internet crimes, with 93,796 victims, followed by Canada and India. An analysis released recently, says that more than one out of every two Indian citizens (59 percent) had been cyber spoken in the previous 1 year, with seven out of ten Indian citizens (of those polled) believing that remote employment made it much easier for hackers and cyber criminals to use it. Another survey found that over 27 million Indian adults have been victims of identity theft in the past 1 year and 52% of Indians feel they are unaware of how to protect themselves from cybercrime.[15]

A police team from other states visits Jharkhand district on a regular basis as one of the primary hotspots of cyber-crime in the country. Between April 2015 and March 2017, policemen from 12 different nations visited the Karmatar police station 23 times and arrested about 38 persons, according to data. Between July 2014 and July 2017, the Jamtara District Police documented more than 80 occurrences involving 330 people in the district. In 2017, the Karmatar police station alone was responsible for almost 100 arrests. In 2011, top police authorities identified the first incidents of online fraud using mobile phone charges. An out-of-district group of youths figured out how to charge phones without paying and made a lot of money quickly. A few years later, there were reports of money being syphoned from bank accounts by getting financial documents.

Year	No. of Cyber Crimes reported
2019	44,546
2018	27,248
2017	21,796
2016	12,317
2015	11,592
2014	9,622
2013	5,693
2012	3,477

[13] Helpline Law, (Date of Publication). “Headline of the article.” Retrieved from https://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india-what-is-types-web-hijacking-cyber-stalking.html (Last accessed 31 May 2021).

[14] Statista, (Date of Publication if available). “India Cybercrime.” Retrieved from https://www.statista.com/statistics/309435/india-cyber-crime-it-act/(Last accessed 31 May 2021).

[15]Norton LifeLock 2021 Norton Cyber Safety Insights Report https://www.statista.com/statistics/309435/india-cyber-crime-it-act/

2.1 Types of Cyber Crimes

Malware Attacks

A malware attack is when a computer system or network is infected with a computer virus or malware of some kind. Hackers may use a malware-infected computer for a variety of purposes. The theft of personal information, as well as the use of computers to commit other crimes or damage data, are examples of these crimes. A noteworthy example of malware attack is the ransomware attack, which was carried out globally in May 2017.[16]

Ransomware is a kind of computer virus that is used to extract money from users by encrypting their data or equipment. WannaCry is a kind of ransomware that exploits a vulnerability in Microsoft Windows computers.230,000 PCs in 150 countries were infected with the malware WannaCry when it first appeared.[17] Users have been locked out of their files, and a notification has been sent out requiring a Bitcoin reservation in order to reclaim access. The WannaCry ransomware attack is estimated to have cost $4 billions throughout the world.

Phishing

A phishing campaign is sending spam emails or other forms of contact to a large number of recipients in order to trick them into doing actions that compromise their security or the security of the organisation for which they work.[18]Contaminated appendices or links to malicious websites might be included in phishing messages. Alternatively, you might ask for the recipient's answer to be kept private. One of the most noteworthy instances of the 2018 phishing scam was the World Cup. E-mails to football fans were included in the World Cup phishing campaign.[19]

The purpose of these phishing letters was to get World Cup fans to visit Moscow for a free trip. Any visitors who looked at these e-mails or followed the links might obtain private info. Phishing may also include spear-phishing. Targeted phishing attacks are made in order to trick employees into endangering their own safety in order to serve the interests of their employer. In contrast to mass phishing attempts in appearance, spear-phishing emails generally look to be from a

[16] https://www.kaspersky.co.in/resource-center/threats/ransomware-wannacry
[17] https://www.kaspersky.co.in/resource-center/threats/ransomware-wannacry
[18] https://www.csoonline.com/article/3234716/8-types-of-phishing-attacks-and-how-to-identify-them.amp.html
[19] Howling, Matt. 2020. “Staying Safe from Cyber-Crime and Scams.”

reliable source. They seem to have come from the CEO or the director of information technology, for example. It's possible that there's no obvious sign that they're not true.

PUPs

PUPS, or Potentially Unwanted Programs, are less hazardous than other types of cybercrime, however malware is one of them. They deinstall the software that is necessary on your machine, which includes search engines and downloaded programmes. Installing antivirus software is a smart idea to avoid dangerous downloads that may include malware or Hardware.[20]

Distribution of Do's attacks

DDoS attacks are a kind of cybercrime in which hackers utilise a distributed denial-of-service (DDoS) attack to bring down a system or network. DDoS attacks are sometimes used to launch attacks using connected IoT devices.[21]A DDoS attack that spams the system with connection requests will overwhelm a system that uses one of the most popular communication protocols. Cyber criminals who engage in cyber-extortion may seek money by using the threat of a DDoS attack. A DDoS attack might potentially be used as a decoy while other criminality is being perpetrated. The DDoS attack on the website of United Kingdom National Lottery in 2017 could be a good example of such attack.[22] As a result, the lottery website and mobile app were down, and British residents were unable to participate.

Botnets

Botnets are networks that are controlled remotely by remote hackers using hijacked computers. These botnets are then used by remote hackers to send spam or launch attacks on other computers. Botnets may also be used for malicious objectives such as spreading malware.[23]

[20] https://www.cybercrimechambers.com/blog-pups-82.
[21] https://www.kaspersky.co.in/resource-center/threats/ddos-attacks
[22] https://www.welivesecurity.com/2017/10/02/uk-national-lottery-ddos-attack/
[23] https://staysafeonline.org/stay-safe-online/identity-theft-fraud-cybercrime/malware-and-botnets

Received: 26.05.2021 – Accepted: 23.06.2021

Cyberstalking

This kind of cybercrime includes online harassment, which occurs when a person receives a large number of online messages and emails. Cyber-speakers, in general, terrify and incite terror through social media, websites, and search engines. The cyberstalker is frequently familiar with the victim and instils anxiety or concern about their safety in them.

Illegal / banned content

Criminals exchange illegal things and disseminate them in a frightening and unpleasant manner. Criminal offenders are included in this online crime. Furthermore, objectionable content may include, but is not limited to, adult sexual activities, violent flicks, and criminal activity films. Materials used in terrorist attacks and materials used to exploit minors are examples of illegal content. On the Internet, this kind of content is distributed via an anonymous network.

Internet Scams

These are typically in the form of advertisements or spam emails that promise unrealistic money or incentives. When you click on an appealing offer that seems "too good to be true," you risk interfering with and compromising viral information. False information when someone assumes your name and says you have access to resources such as credit cards, bank accounts, and other advantages, this is known as identity theft. [24]It's possible that you'll utilise your alias to commit other crimes. Credit card fraud is a wide term that refers to identity theft crimes in which the perpetrator uses your credit card to pay for his transactions. Credit card fraud is the most basic kind of identity theft. The most common kind of card fraud occurs when your pre-approved card falls into the wrong hands.

[24] Boussi, Grace Odette, and Himanshu Gupta. 2020. "A Proposed Framework for Controlling Cyber- Crime." In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 1060–63.

Exploiting Toolkit

To get access to a user's control, operation kits need a vulnerability (software code flaw). They are ready-made tools that criminals may purchase and employ against anybody using a computer and a computer. The exploit kits are updated on a regular basis, much like regular software.

2.2 Challenges in India’s Cyber Security Approach

Lack of Cybersecurity Personnel in the Indian Military, Central Police, Law Enforcement Agencies, and Other Organizations: The Indian military, central police, law enforcement agencies, and other organisations all lack staffing in this area for software and hardware aspects. Furthermore, the need for Artificial Intelligence (AI), Block Chain (BCT), Internet of Things (IoT), and Machine Learning skills is growing (ML).

According to some estimates, there is now a need for at least 3 million cybersecurity professionals. Active cyber defence: Unlike the GDPR and the Clarifying Lawful Overseas Use of Data Act, India does not have “active cyber defence” (CLOUD).[25]Regulatory Intersections: Unlike the United States, Singapore, and the United Kingdom, where a single paraglider organisation is responsible for cyber security, India has a variety of central agencies responsible for cyber concerns, each with its own reporting structure.

- Every government also has its own cyber-response squad.
- Dependence on Foreign Players For Cyber Security Technologies: India has no indigenous usage of hardware or cybersecurity technologies.
- As a result, India’s cyberspace is vulnerable to both state-sponsored and non-state-sponsored cyberattacks.

Other difficulties include the fact that social media is becoming an important means of disseminating information, making it more difficult to distinguish between true and false news. Increased Chinese influence in Indian telecommunications is one example of a challenge.

[25] Sarker, Iqbal H., Yoosef B. Abushark, Fawaz Alsolami, and Asif Irshad Khan. 2020. “IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model.” Symmetry 12 (5): 754.

2.3 Prospective change in Govt. approach

- The Awareness: With a nation using digital warfare and hackers to target commercial organisations and government activities, India must raise awareness that no one person or institution is immune.
- While the government and the corporate sector may be better placed to formulate their own strategies, it is civil society that must bring about this change.
- Increasing the effectiveness of the present cyber security architecture. Several national cybersecurity programmes, such as India's Cyber Coordination Centre, the National Critical Information Infrastructure Protection Platform, and CERT, need strengthening and changes.
- Bringing cyber security into the classroom: Educational institutions such as Central Universities, private universities, business organisations, and it is should all provide cyber security programmes.
- TO THE INTEGRATED APPROACH: As the mobile and telecommunications domains continue to grow in importance, national cyber-security and national telecom policy will need to collaborate to establish a comprehensive 2030 plan.
- The Promotion of Indigenization: It is necessary to establish opportunities for developing software for cyber security and digital communications.
- The Indian government may consider including cyber security architecture as part of its Make In India plan.
- In addition, creating a customised Indian template that may meet localised expectations necessitates the creation of corresponding hardware.

2.4 Toolkit for Cyber Security

The deployment of software to protect your networks and systems serves as a deterrent to hackers who prefer to target easier targets that need less effort and are less hazardous. Although no programme can be guaranteed to be impenetrable 100 percent of the time, cyber thieves' construction of access holes makes security software more difficult to crack and is seen as an extra layer of protection against hackers.[26]

[26] Boussi, Grace Odette, and Himanshu Gupta. 2020. "A Proposed Framework for Controlling Cyber- Crime." In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 1060–63.

Antivirus software

Malware is detected and removed by antivirus software, which also stops it from accessing the system in the first place. Malware is any piece of software that has the potential to do harm (or malicious software). When we hear about Trojan horses, spyware, ransomware, viruses, and other forms of malware, we're talking about malware. [27] Antivirus software works by scanning your computer on a regular basis and systematically eliminating previously installed malicious pieces. It also looks for potentially dangerous files in emails or direct messages and alerts or deletes them before they may cause harm. Because of the ongoing advancements in malware, it is critical that antivirus software be updated on a regular basis to be secure.

Firewalls

Firewalls, which block specific types of network traffic and provide protection against unsustainable networks, are the first line of defence. Firewalls operate by continuously monitoring network traffic on your device and rejecting connection requests from any source that it considers to be hazardous. It acts as a filter, deciding what enters and exits your network, and providing you with an extra layer of protection in addition to antivirus software.

- Firewalls have a set of rules that govern what is allowed and what is not. A list of rules is available on certain firewalls.
- Stateful firewalls are similar to packet filters for firewalls, but they have a little advantage in terms of keeping track of active connections.
- A thorough analysis of the packs Firewalls examine the content of data packets, allowing them to differentiate between attacks and normal access.
- Deep-packet-inspection firewalls are similar, but smarter and capable of determining if particular processes are risky or benign.
- Proxy applications on firewalls intercept and validate traffic (e.g., email, web traffic, etc.) before allowing it to proceed.

[27] Chatterjee, Sheshadri, Arpan Kumar Kar, and M. P. Gupta. 2018. "Alignment of IT Authority and Citizens of Proposed Smart Cities in India: System Security and Privacy Perspective." Global Journal of Flexible Systems Management 19 (1): 95–107.

Users should never deny or disdain attempts to update themselves through security software, just as they should never reject or disrespect efforts to update themselves using antivirus-based software.[28]

Encryption

Encryption is a complicated algorithm that employs data conversion techniques. Users need a key to quickly access vital information (decryption algorithm). Because unauthorised persons do not have the necessary key, data encryption reduces the chances of unauthorised persons accessing and using it. This kind of security is often used while sending or storing data on mobile devices via the Internet.[29]

Staff training

Cyber security expertise is essential for protecting your systems. A single individual's lack of comprehension might have a ripple effect across your network. As a result, every employee must be thoroughly trained and refreshed on a regular basis. By human error, the door is regularly left open to intruders. Although no human error can ever be completely eliminated, a solid understanding of strong protections and the importance of conformance may help to close gaps. Because cyber security threats are always evolving, it's critical to keep up with the latest information on current protection and to refresh your cyber security skills on a regular basis.

To have a better grasp of cybersecurity, one must follow these steps.[30]

- When providing personal information, always use trustworthy websites. The URL is a good guideline to follow. This is a wonderful rule. If the website utilises https://, it is considered secure. Do not enter sensitive personal details like credit card no. or Social Security numbers if the URL has the http:// — note the missing s.[31]

[28] Shah, Pintu, and Anuja Agarwal. 2020. "Cybersecurity Behaviour of Smartphone Users in India: An Empirical Analysis." In Information & Computer Security, 28:293–318.

[29] Chatterjee, Sheshadri, Arpan Kumar Kar, and M. P. Gupta. 2018. "Alignment of IT Authority and Citizens of Proposed Smart Cities in India: System Security and Privacy Perspective." Global Journal of Flexible Systems Management 19 (1): 95–107.

[30] Howling, Matt. 2020. "Staying Safe from Cyber-Crime and Scams."

[31] Chatterjee, Sheshadri, Arpan Kumar Kar, and M. P. Gupta. 2018. "Alignment of IT Authority and Citizens of Proposed Smart Cities in India: System Security and Privacy Perspective." Global Journal of Flexible Systems Management 19 (1): 95–107.

- Do not open email attachments or emails that include email links from unknown sources. Emails masquerading as being provided by someone you trust are one of the most common ways of exposing networks and individuals to malware and viruses.
- One should Keep one's electronics up to date at all times. Upgrades to software deliver critical vulnerability patches. Cyber criminals may also target devices that are out of date and do not have the most up-to-date security software.
- We should Back up our data on a regular basis to ensure security in the event of a cyber security incident. If you need to wipe your device clean due to a cyber attack, it will aid you in saving your data separately and securely.

2.5 Cyber Security Laws in India

2.5.1 National Cyber Security Policy

It is a mechanism to deal with digital and information technology by the Electronics and Information Technology Department. The main goal of the Cyber Security programme is to defend the public and private systems against cyber threats. To prevent this data from falling into the wrong hands, the government wants to secure "personal details (such as online users' data), banking and financial data, and sovereign data. Internet is a complex ecosystem that involves people, application programs, and widespread dissemination of information and communication technology.[32]Need for a cybersecurity policy:

- Before 2013, India did not have a cybersecurity policy. The need for it was felt during the NSA spying issue that surfaced in 2013.[33]
- Information empowers people and there is a need to create a distinction between information that can run freely between systems and those that need to be secured. This could be personal information, banking and financial details, security information which when passed onto the wrong hands can put the country's safety in jeopardy.
- This rule has been drafted by consulting all the stakeholders.

[32] Legal Service India, (Date of publication), "An analysis on cybercrime in India." Retrieved from http://www.legalserviceindia.com/legal/article-797-an-analysis-on-cyber-crime-in-india.html(Last accessed 31 May 2021).

[33] https://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india-what-is-types-web-hijacking-cyber-stalking.html

Received: 26.05.2021 – Accepted: 23.06.2021

- In order to digitise the economy and promote more digital transactions, the government must be able to generate trust in people in the Information and Communications Technology systems that govern financial transactions.
- A strong integrated and coherent policy on cybersecurity is also needed to curb the menace of cyber terrorism.

2.5.2 Indian Cyber Crime Coordination Centre

In October 2018, the plan to establish I4C was authorised, with the goal of dealing with all sorts of cybercrime in a comprehensive way.[34]

It has seven components:

1. National Cyber Crime Threat Analytics Unit (NCC-TAU)
2. NCC Reporting Portal
3. NCC Training Centre
4. Cyber Crime Ecosystem Management Unit
5. NCC - Research and Innovation Centre
6. NCC Forensic Laboratory Ecosystem
7. Joint Cyber Crime Investigation Force.

15 States along with the Union Territories have approved the consent to lay up Regional Cyber Crime Coordination Centres.

2.5.3 National Cyber Crime Reporting Portal

It is a public-focused initiative that enables anyone to report cyber crimes via Internet, and the applicable law enforcement agencies will review all complaints and take appropriate action as required by law. The website focuses mostly on women's crimes, as well as children's crimes, including child pornography, child abuse materials, rape and gang rapes, and online materials, among other things.[35]

It also focuses on financial crimes and related social media crimes like harassment and cyber intimidation, among other things. The site was officially launched on August 30, 2019.Improved

[34] Shivangi, Saumya. 2020. "India : Challenges and Threats Regarding National Security." Shodhshauryam International Scientific Refereed Research Journal 3 (1): 163–65.

[35] Shah, Pintu, and Anuja Agarwal. 2020. "Cybersecurity Behaviour of Smartphone Users in India: An Empirical Analysis." In Information & Computer Security, 28:293–318.

collaboration between law enforcement authorities in different states, and police stations would increase the capacity of police agencies to effectively investigate crimes.[36]

2.5.4 National Critical Information Infrastructure Protection Centre (NCIIPC)

The National Infrastructure Protection Centre was established by a gazette notice with specific duties to preserve each CII (NCIIPC). CERT-IN would be in charge of non-critical systems, but would continue to report on hacks and events. All non-critical systems are under the control of the CERT-IN team. It took six years for the laws to be changed in 2008 before the NCIIPC was formally established in January 2014 by a Government of India statement.[37]

NCIIPC started with a variety of sectors, but has since narrowed its focus to five "important sectors". The following are some examples:

- Energy and Power are two terms used interchangeably.
- Banking, financial insurance, and financial institutions are all examples of financial institutions.
- Information and communication technology (ICT)
- Transportation Modes of transportation
- E-governance and strategic public businesses

While defence and intelligence organisations were included in the CII structure, they were kept outside of the NCIIPC's charter's authority. Instead, the DRDO has been tasked with keeping watch on these corpses. The DRDO is a defence research and development organisation.

2.5.5 Cyber Swachhta Kendra

A component of India's administration's digital initiative to protect the cyber domain by discovering botnet invasions in China and alerting, mopping, and securing users' computers from new infections is the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). This

[36] Shivangi, Saumya. 2020. "India : Challenges and Threats Regarding National Security." Shodhshauryam International Scientific Refereed Research Journal 3 (1): 163–65.

[37] https://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india-what-is-types-web-hijacking-cyber-stalking.html

initiative is under the jurisdiction of the Ministry of Electronics and Information Technology (Meit Y). In line with the National Cyber Security Policy, which directs the development of a safe cyber ecology in the country, the "Cyber Swachhta Kendra" was founded (Botnet Cleaning Centre and Malware Analysis Centre). The centre works very closely with ISPs, products, and viruses, and they also interact with each other. This page offers helpful tips and resources to help keep computers and gadgets safe. This facility is formed under Section 70B of the Information Technology Act, 2000, that gives the Indian Computer Emergency Response Team (CERT-IN) jurisdiction. (CERT-I).[38]

2.5.6 The Information Technology Act of 2000

An IT Act was submitted to the Indian Parliament on October 17, 2000. The IT Act is based on the UN General Assembly's Resolution 30 January 1997, which advocated for the adoption of the UNCITRAL Model Law for Electronic Commerce. India has a high-value cybercrime and e-commerce law.[39]

The primary goal of this Act is to deal lawfully and reliably with electronic, digital, and online transactions, as well as to eradicate or reduce cybercrime. The IT Act is divided into 13 chapters with a total of 90 chapters. The following five portions, beginning with section 91 and ending with paragraph 94, deal with the Indian Penal Code 1860 amendments.[40]

1. Section 65 - This section applies to the unauthorised alteration, theft, or loss of computer source materials. It is created to be used to conceal, corrupt, or remove computer source code for a computer, computer programmes, computer system, or computer network. fines up to ₹. 200,000, or a sentence of jail for up to three years.
2. Section 66 - Hacking someone's computer system: Hacking occurs when someone aims to cause or knows that he or she may cause illegal public losses or harm, or when someone destroys, alter, or edits any data stored in a computer resource, or reduces its worth, or damages it in any way. Up to 3 years in jail or a fine of up to ₹ 500,000 is the penalty.
3. Section 66A – Publishing something offensive, wrong or threatening info's: To cause annoyance, discomfort, danger, or injury, anyone who sends any information via an electronic computer resource that is seriously offensive or threatening, or anything of information she/he

[38] Shrivastava, Gulshan, Kavita Sharma, Manju Khari, and Syeda Erfana Zohora. 2018. "Role of Cyber Security and Cyber Forensics in India." In, 1349–68.
[39] Bommakanti, Kartik. 2020. "India's Cyber Defence Capabilities."
[40]Indian Penal Code 1860 am. 69,70,72

knows which could be false, is subject to a sentence of imprisonment of up to three years and a fine.

4. Section 66B – Receiving computer which is stolen or any other communication device: A computer or communication device is handed or maintained to a person who has previously been robbed or stolen. Criminality carries a sentence of up to three years in prison and/or a fine of up to ₹ 100,000.
5. Section 66C - Using password or security code of another person: A fraudster uses another person's password/security code, digital signature, or some other unique personal identity to commit fraud. Penalty: three years in jail or a fine of up to ₹ 1,00,000.
6. Section 66D – Cheating or fraud activity using compute/electronic resource: If someone defrauds another person via the use of a computer or other means of communication. Criminality carries a sentence of up to three years in prison and/or a fine of up to RS 100,000.
7. Section 66E –Posting someone's private images: When a person takes, transmits, or publishes images of a person's private parts without that person's consent or knowledge. Penalty: imprisonment for up to three years or a fine of up to ₹ 2,00,000.
8. Section 66F - Cyber terrorism: Cyber-terrorism happens when a person restricts authorised personnel access to a computer resource, accesses a secured system, or introduces pollutants into a system in order to jeopardise India's unity, integrity, sovereignty, or safety. Criminality carries a sentence of life in jail.
9. Section 67 – Posting something obscene on Internet: If a person publishes, transmits, or causes to be published electronically, all material that is laciest or that appeals to prudent interest or has the effect of depraving and corrupting persons who are likely to read, see, or hear the matter contained in or embodied in that material in light of all relevant circumstances is prohibited. Penalty: up to five years in prison or a fine of RS 1.000.000 Penalty: up to five years in jail or a fine of ₹ 1,000,000.
10. Section 67A - Publishing images containing sexual acts: It is a criminal offence to published or share image of a sexual activity or behaviour that is explicit. Penalty: Seven years in prison or a fine of up to ₹ 10 lakh.
11. Section 67B -Posting child pornography or predating a child on Internet: When a person intentionally captures, publishes, or transmits a child's images in a sexually explicit manner. If someone encourages a child to engage in sexual activity, it is considered child abuse. Any person under the age of eighteen is referred to as a child. Penalty: Up to a five-year jail sentence or a fine of up to RS 1000 000 on the first conviction. For a second conviction, a

prison cam be sentenced up to seven years may be imposed, as well as a fine of up to ₹10,00,000.

12. Section 67C - Failing to keep records: For a set length of time, intermediate (e.g. ISPs) must keep records. Violation is defined as an infringement. Punishment—Up to three years in prison or a fine.
13. Section 68 – Failure to go by orders: By order, the Controller may, if necessary, direct a certifying authority and any employee thereof to adopt or halt such steps to ensure that the terms of this Act are complied with, or regulations therein enacted may be adopted. The Controller may do so by order. Anyone not executing such directives is responsible for an offence. Criminal offences: up to three years in prison or up to ₹ 2,00,000 in fine.
14. Section 69 – Failure to decrypt information: If the Controller is satisfied that intercepting any information is necessary or expedient in the interests of India's sovereignty or integrity, for reasons that must be documented in writing, any state wing may intercept any data for the purposes of State security, foreign relations with foreign countries, or public order, or to prevent incitation to commit any recognisable crime, any government agency may intercept any information by order. When a directorate requests it, the subscriber or anybody responsible for the computer resource shall provide all of the important facilities and technological help to decrypt the data. It is considered a criminal offence for a subscriber or anybody who does not support the aforementioned agency. Penalty - Up to 7 years in jail and a fine.
15. Section 70 - Attempting access to any protected system: A secured system of any computer system, PC or some computer network may be declared by informing the government in the Official Gazette. By written order, the government in question may let those who have been granted access to protected systems. An infringement occurs when someone gains breach to a protected system or attempts to get access to one. Penalty: up to ten years in jail or a fine of up to $10,000.
16. Section 71 – Misrepresentation Criticism: In order to get a licence or a digital signature certificate, someone misrepresents the controller or the certifying authority, or eliminates any important details from it. Criminality is the act of committing crimes. Up to three years in prison or an RS 100,000 fine are possible penalties.

3. Conclusion

Individuals in the community and the workforce must be aware of cyber security and get training that is supported by relevant learning theories in order to produce people who are capable of mitigating current and future cyber attacks. As a result, if consumers and the workforce are appropriately educated and trained to adopt essential safeguards to deal with difficulties related to digital privacy and security, there will be an improvement in cyber security. Insufficient staff and the larger workforce, on the other hand, seem to be failing to understand how to manage cyber security and respond appropriately to cyber attacks.[41] There seem to be no effective cyber security measures in place for people and the current workforce.

In our world today, digitisation is on the rise and the Internet has simplified our lives. It's everything at our fingertips with only a simple tap. The total number of cyber – crimes in India has also grown, particularly from white-collar crimes and terror attacks. Using technologies has rendered humans totally reliant on it for their fundamental needs. Today we must meet all of our needs online much as in an internet shopping or buying restaurant meals, playing games, making financial transactions, and so on. To address the challenge of such crimes, governments, the tech sector, security groups, IT businesses, and internet service providers should all come together to develop holistic partnerships.

References

Bommakanti, Kartik. 2020. "India's Cyber Defence Capabilities."

Boussi, Grace Odette, and Himanshu Gupta. 2020. "A Proposed Framework for Controlling Cyber-Crime." *In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO),* 1060–63.

Business Standard, "Current Affairs". https://www.google.com/amp/s/wap.business-standard.com/article-amp/current-affairs (Last accessed 02 June 2021)

Ch, Rupa, Thippa Reddy Gadekallu, Mustufa Haider Abidi, and Abdulrahman Al-Ahmari. 2020. "Computational System to Classify Cyber Crime Offenses Using Machine Learning." *Sustainability* 12 (10): 4087.

Chatterjee, Sheshadri, Arpan Kumar Kar, and M. P. Gupta. 2018. "Alignment of IT Authority and Citizens of Proposed Smart Cities in India: System Security and Privacy Perspective." *Global Journal of Flexible Systems Management* 19 (1): 95–107.

Cyber Crime Chambers, https://www.cybercrimechambers.com/blog-pups-82 (Last accessed 02 June 2021).

[41] Rupa et al., 2020. "Computational System to Classify Cyber Crime Offenses Using Machine Learning."

Helpline Law, “Employment Criminal and Labour” https://www.helplinelaw.com/employment-criminal-and-labour (Last accessed 02 June 2021).

Howling, Matt. 2020. “Staying Safe from Cyber-Crime and Scams.”

Humayun, Mamoona, Mahmood Niazi, NZ Jhanjhi, Mohammad Alshayeb, and Sajjad Mahmood. 2020. “Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study.” *Arabian Journal for Science and Engineering* 45 (4): 3171–89.

Kanakam, Prathyusha, and Asn Chakravarthy. 2020. “Packet Crafting Tools for Cyber Crime Security Attacks.” *International Journal of Computer Applications* 176 (31): 28–30.

Kaspersky, “DdoS Attacks.” https://www.kaspersky.co.in/resource-center/threats/ddos-attacks (Last accessed 02 June 2021).

Legal Service India, “An analysis on Cybercrime in India” Retrieved from http://www.legalserviceindia.com/legal/article-797-an-analysis-on-cyber-crime-in-india.html (Last accessed 02 June 2021)

Patel, Durgambini A., and Sanjana Bharadwaj. 2020. “The Code on Social Security in India, 2019.”

Rastogi, Neha, and Pradeep Chauhan. 2020. “Providing Security &Minimizing Fake Calls by Use of Hashing Algorithm in Digital India.” *In 2020 International Conference on Intelligent Engineering and Management (ICIEM).*

Sahoo, Subham, Tomislav Dragicevic, and Frede Blaabjerg. 2020. “Cyber Security in Control of Grid-Tied Power Electronic Converters–Challenges and Vulnerabilities.” *IEEE Journal of Emerging and Selected Topics in Power Electronics,* 1–15.

Sarker, Iqbal H., Yoosef B. Abushark, Fawaz Alsolami, and Asif Irshad Khan. 2020. “IntruDTree: A Machine Learning Based Cyber Security Intrusion Detection Model.” *Symmetry* 12 (5): 754.

Shah, Pintu, and Anuja Agarwal. 2020. “Cybersecurity Behaviour of Smartphone Users in India: An Empirical Analysis.” *In Information & Computer Security,* 28:293–318.

Shivangi, Saumya. 2020. “India : Challenges and Threats Regarding National Security.” *Shodhshauryam International Scientific Refereed Research Journal* 3 (1): 163–65.

Shrivastava, Gulshan, Kavita Sharma, Manju Khari, and Syeda Erfana Zohora. 2018. “Role of Cyber Security and Cyber Forensics in India.” In, 1349–68.

Statista, “India: Cyber Crime” Retrieved from https://www.statista.com/statistics/309435/india-cyber-crime-it-act (Last accessed 02 June 2021).

The Hindu, “Technology” https://www.thehindu.com/sci-tech/technology (Last accessed 02 June 2021).

Vijai, C. 2020. “Cloud-Based E-Governance in India.” Social Science Research Network.

We Live Security, (02 October 2017), “UK National lottery DdoS Attach.” Retrieved from https://www.welivesecurity.com/2017/10/02/uk-national-lottery-ddos-attack/(Last accessed 02 June 2021).

Yadav, Tarun Kumar, Akshat Sinha, Devashish Gosain, Piyush Kumar Sharma, and Sambuddho Chakravarty. 2018. “Where The Light Gets In: Analyzing Web Censorship Mechanisms in India.” *In Proceedings of the Internet Measurement Conference 2018 On,* 252–64.

Yang, Bo, Hongxin Hu, and Yunyun Xie. 2020. “A Review on Cyber Security of Digital Electro-Hydraulic Control System of Steam Turbine.” *In 2020 IEEE 4th Conference on Energy Internet and Energy System Integration (EI2).*