STUDY ON CYBERCRIMES IN SOUTH-ASIAN COUNTRIES

Rishabh Jain[1]

INTRODUCTION

Every element of human life has been transformed by the information and communication technology (ICT) age, which includes email, the internet, mobile phones, satellites, and social networking sites. Currently, the internet has developed into a significant symbol of the digital age, especially in cyberspace. The importance of people, organizations, interest groups, social movements, and international networks has expanded in the information or digital age. A nation's technical infrastructure is continually in danger, and this puts the national security sector under constant pressure.

The dangers span a wide range of topics, including privacy concerns, critical infrastructure protection, cybercrime, cyberterrorism, and cyber hazards. The globe is now more interconnected as a result of our growing reliance on technology, which has also caused the computer industry to grow and the number of internet hosts to increase. The internet and information and communication technologies (ICTs) play a crucial role in socioeconomic development. Information technology is now used by governments, economies, and communities to carry out crucial tasks. However, the internet is no longer secure because to its enormous accessibility. The digital revolution has highlighted concerns about security and privacy, particularly the idea of cyber security.[2]

New technology-related threats are rapidly expanding and changing all the time. They occasionally have goals other than financial gain and are started by non-state actors through a variety of sources, including political organizations and foreign powers. They could be any form of "hacktivism" for military purposes, cyber espionage, sabotage (like Stuxnet), or even destabilization (as in Estonia in 2007).[3] Cyberattacks are well-planned and have become substantially more sophisticated over time, as shown by the

[1] Law Student, 4th Year, B.A.LL.B., Faculty of Law, Vivekananda Global University, Jaipur.
[2] Laura DeNardis, *A HISTORY OF INTERNET SECURITY* (The History of Information Security: A Comprehensive Handbook 2007) 681-704
[3] OECD, 'Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for The Internet Economy' (*OECD*, 2012) <https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf> assessed 20 November 2022

sophistication of cybercriminals, the advent of cyber espionage, and the well-publicized operations of hacker collectives. These are unmistakable evidence of professionalism. In light of this context, a number of nations have identified cybersecurity as one of the most important security concerns for both the present and the future.[4] Cybersecurity is now a crucial part of national strategy and must be tackled holistically, taking into account diplomatic, economic, educational, intelligence, law enforcement, legal, military, social, and technical factors.[5]

RELATION BETWEEN INDIA AND SOUTH ASIAN NATIONS

The SAARC Charter was ratified in Dhaka on December 8, 1985, establishing the South Asian Association for Regional Cooperation (SAARC). Afghanistan, Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan, and Sri Lanka are the eight members of SAARC. On January 17, 1987, the Association's Secretariat was established in Kathmandu.

The objectives of the Association as outlined in the SAARC Charter are: to promote the welfare of the peoples of South Asia and to improve their quality of life; to accelerate economic growth, social progress, and cultural development in the region and to provide all individuals the opportunity to live in dignity and to realize their full potentials; to promote and strengthen collective self-reliance among the countries of South Asia; to contribute to mutual trust, understanding and appreciation of one another's problems; to promote active collaboration and mutual assistance in the economic, social, cultural, technical and scientific fields; to strengthen cooperation with other developing countries; to strengthen cooperation among themselves in international forums on matters of common interests, and to cooperate with international and regional organizations with similar aims and purposes.[6]

[4] Myriam Dunn Cavelty, 'The Militarisation of Cyber Security as a Source of Global Tension' (2012) STRATEGIC TRENDS ANALYSIS: Center for Security Studies 103 < https://www.researchgate.net/publication/228192669_The_Militarisation_of_Cyber_Security_as_a_Source_of_Global_Tension> assessed 20 November 2022

[5] OECD, 'Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for The Internet Economy' (*OECD*, 2012) <https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf> assessed 20 November 2022

[6] 'About SAARC' (*SAARC*, 12 July 2020) <https://saarc-sec.org/index.php/about-saarc/about-saarc> assessed 20 November 2022

To ensure security from regional social ills like terrorism, drug trafficking, trafficking in children and women, and transnational crimes, SAARC has put into place a number of directives. In numerous SAARC meetings, it was highlighted that while denouncing terrorism in all of its forms and manifestations, there should be no exceptions for terrorists in the criminal justice system. In order to combat transnational organized crime, provide safety and security for social and economic growth, and particularly create a secure future for children, women, and young people, it is essential to come up with effective solutions. In order to combat these widespread societal ills within the area, SAARC is working to strengthen the monitoring system, information exchange, and technological interchange.[7]

Hence it is important for us to study the cybercrimes in India as well as other south Asian nations to determine how far is India ahead or in line with its neighboring nations. The present article focuses on the issue of cyber security and crimes in South Asian Nations (Pakistan, Sri Lanka, Bangladesh, Nepal, and Afghanistan) in comparison with India and the cyber laws of all those nations.

CYBER SECURITY: A GROWING CONCERN FOR INDIA

In the current day, cybersecurity has risen to the top of a long list of diverse issues. The "next generation of threats" is now thought to be emerging in the cyber domain. India is one of the top five countries targeted by harmful online activity, which includes anything from identity theft to spamming, viruses, and web defacement to denial-of-service attacks, email bombing, hacking, and cyber slander. From 23 in 2004 to 2,565 in 2008 to 10,315 in 2010 to 13,301 in 2011 and 62,000 up to mid-2014, the number of cyberattacks has been gradually increasing.[8]

Cybersecurity has taken on significance in national security issues in the digital age as ICT has integrated with Indian industry and governance. Cyberattacks always have a chance to compromise the security of the things they target, whether they be people, companies, or governments. Systems that support the nation's vital intelligence and defense communities are likewise susceptible to similar attacks. Therefore, all

[7] 'Education Security and Culture' (*SAARC*, 16 July 2020) <https://saarc-sec.org/index.php/areas-of-cooperation/education-security-culture> assessed 20 November 2022

[8] N Manoharan, 'India's Internal Security Situation: Threats and Responses' (2013) 69(4) India Quarterly: A Journal of International Affairs 367–81

cyberattacks, whether directed at people, companies, or government institutions, have grave repercussions, with attacks on the government apparatus bearing a heightened risk of the theft of military and state secrets.[9]

In the context of India, crucial industries such as defense, energy, finance, telecommunication, transport, and other public services primarily rely on networks to convey data for communication and business operations. Internet use in these fields serves as a communication and information source and is important for maintaining national security. The government has grand plans to improve communication channels, cyber connectivity, and e-commerce services. The comprehensive Digital India program, which aims to promote e-governance, connect all gram panchayats (village councils) to broadband internet, and transform India into a connected knowledge economy, has been approved by the cabinet, according to Prime Minister Narendra Modi.[10] Therefore, the government must adopt strong policies to cope with cyberattacks and provide security to all sectors.[11]

CYBER CRIMES IN INDIA

In a report, Economic Times[12] mentions that in Bengaluru (the cyber-crime capital of India), 8 new police stations for cyber-crimes were announced in December 2018 to handle the growing number of cyber-crime cases in Bengaluru. Cyber cases registered in India are increasing rapidly. In India, 80% of adults that is, 4 out of 5 adults were victimized by cybercrime, the reason behind this might be the high usage and less literacy rate of E-commerce. More than 46 million users are using online shopping, e-commerce, and social networking sites.[13] Table III depicts how the various state of India is affected

[9] SRR Aiyengar, *National Strategy for CyberSpace Security* (New Delhi: KW Publishers 2010)
[10] PTI, 'Most cyberattacks on India show Chinese IP address: NTRO' (*The Indian Express*, 13 November 2014) <https://indianexpress.com/article/india/india-others/most-cyber-attacks-on-india-show-chinese-ip-address-ntro/> assessed 20 November 2022
[11] Anoop Kumar Verma & Aman Kumar Sharma, 'Cyber Security Issues and Recommendations' (2014) 4(4) International Journal of Advanced Research in Computer Science and Software Engineering 629–34
[12] Tushar Kaushik, 'Bengaluru is India's cybercrime capital' (*The Economic Times*, 31st January 2019) <https://economictimes.indiatimes.com/tech/internet/bengaluru-is indias-cybercrime-capital/articleshow/67769776.cms?from=mdr.> assessed 20 November 2022
[13] Raja Sarath Kumar Boddu and Venkata Ramana Bendi, 'Cyber Crime and Security, a Global Vulnerable Coercion: Obstacles and Remedies' (2017) 7(5) IJIEE 132 <http://www.ijiee.org/vol7/676-IE010.pdf> assessed 20 November 2022

by cyber-crimes in the duration of 2014-2016. Maharashtra and Uttar Pradesh are the most affected states of India.

CASE STUDIES

- *Extortion case experienced at Greater Hyderabad Municipal Corporation (GHMC)*[14]

At Hyderabad, a data entry operator of GHMC was caught by cyber-crime cops along with his sibling for unscrupulously issuing Property Tax Identification Number (PTIN) for a plot at Rajendra Nagar. An outsource worker named Jay Chand Velaga, earlier logged into the website of GHMS and dishonestly changed the data and issued a door number and PTIN for property for some benefit, his brother assists him in this illegal transaction.

- *Digital Fraud instances of 2017*[15]

An online scam of Rs 3700 crore was registered against a so-called entrepreneur who had fraud almost 7 lakh people in the name of "Social Trade". ICICI Bank Aadhar scam worth Rs 1.3 lakh registered due to panic of linking Aadhar with a bank account. Unauthorized persons pose as bank officials and fooled bank customers by taking their OTP. LIC had been warned regarding the Aadhar scam. Some fraudsters are creating a fake websites to fool LIC customers so that they can fraud their money.

- *Mobile Banking Fraud Cases*

Mobile banking essentially means the bank will have a webpage through which it can almost provide all services of a bank to the customers. Customers sitting at a remote location utilizing their smartphone or laptop can avail of the services of banks like transfer of funds, recharge, payment, etc. As this application is very user-friendly so the number

[14] Aditi Mallick, 'GHMC outsourced staff held for fraud' (*The Times of India*, 06 July 2019) <https://timesofindia.indiatimes.com/city/hyderabad/ghmc-outsourced-staff-held-for-fraud/articleshow/70098538.cms> assessed 20 November 2022

[15] PTI, 'Over 900 cases of fraud involving cards, net banking registered in Apr-Sep 2018' (*The Economic Times*, 13 February 2019) <https://economictimes.indiatimes.com/industry/banking/finance/banking/over-900-cases-of-fraud-involving-cards-net-banking-registered-in-apr-sep-2018/articleshow/67977230.cms> assessed 20 November 2022

of users is also increasing.[16] Recently banks with mobile banking are experiencing very complicated online services since digital privacy and security are on high alert. Therefore, banks are required to provide more secure and safe online banking services.[17] Identity thieves, money launderers, and hackers are focused on various channels and creating new types of attacks so that they cannot be easily trapped by traditional fraud detection systems.[18] Bank customers are now using fewer services of online banking since the number of fraud instances is increasing.[19]

Researchers are going on cyber-crimes to identify the geographical location where maximum instances of cyber-crimes are experienced so that major steps to reduce crimes can be imposed on that area. Additionally, explore of cyber security is likewise occurring for inventing new effective and efficient techniques to countermeasure cybercrimes. Similarly, awareness programs are taking place for alerting people regarding cyber-crimes and various cybersecurity strategies which they can use to prevent or avoid cyber-crimes. Correspondingly traditional networks are replaced by Software Defined Networks (SDN) for making the network more secure.[20] Government is also additionally expanding the number of cyber cells to minimize cyber crimes.

CYBER SECURITY AND SMART CITIES IN INDIA

A smart city is an urbanized area where "numerous sectors cooperate to achieve sustainable outcomes through the analysis of contextual real-time information shared among sector-specific information and operational technology systems".[21] The idea of

[16] Emad Abu-Shanab & Salam Matalqa, 'Security and Fraud Issues of E-banking' (2015) 2(4) IJCNA 179 <https://www.academia.edu/33450273/Security_and_Fraud_Issues_of_E_banking> assessed 20 November 2022

[17] Mitaali Jayant Gilbile & S S Mane, 'A Review on Comparative Study on the Structural Analysis and Design of Pre-Engineered Building [PEB] with Conventional Steel Building [CSB]' (2020) 9(9) IJERT 56 <https://www.ijert.org/research/a-review-on-comparative-study-on-the-structural-analysis-and-design-of-pre-engineered-building-peb-with-conventional-steel-building-csb-IJERTV9IS090028.pdf> assessed 20 November 2022

[18] Krishna Modi and Reshma Dayma, 'Review on Fraud Detection Methods in Credit Card Transactions' (2017) International Conference on Intelligent Computing and Control (I2C2) 103

[19] Rashad Yazdanifard, et al., 'ELECTRONIC BANKING FRAUD: THE NEED TO ENHANCE SECURITY AND CUSTOMER TRUST IN ONLINE BANKING' (2011) 3 IJAISSS 505-509

[20] Vidhu Baggan & Surya Narayan Panda, 'Enhancing Network Path Restoration With Software Defined Networking' (2019) 14(8) IJAERV 1910-1916 <https://www.ripublication.com/ijaer19/ijaerv14n8_21.pdf> assessed 20 November 2022

[21] Marin Ivezic, 'Cyber – A necessary pillar of Smart Cities' (*5G.Security*, 18 November 2016) <https://5g.security/5g-edge-miot-cybersecurity/cybersecurity-pillar-smart-cities/> assessed 20 November 2022

"smart cities" is a relatively new phenomenon, and significant time and money have been invested in creating numerous connected technology application areas. Such initiatives are a response to a number of issues related to densely populated metropolitan regions, with the main goal of improving the quality of life for those who live there.[22]

These cities are additionally susceptible to cyber dangers, as evidenced by a number of incidents. In 2011, a cyberattack on a city water station in Springfield, Illinois, the US, resulted in the destruction of a water pump.[23] Cyber attackers who chose Dallas (Texas) as their target in 2017 took over control of the city's warning sirens and turned them on for several hours at night. Denis Legezo, a Kaspersky Labs employee, demonstrated how to hack into traffic lights in the heart of Moscow and take full control of the system.[24]

The "Smart Cities Mission" was launched by the Indian government to promote local development and enhance people's quality of life while utilizing technology to produce intelligent outcomes for citizens. The administration has been working to develop 100 smart cities in this direction. India is more susceptible to cyberattacks, though, as it is still in the early stages of creating its cyber security infrastructure and lacks the qualified personnel needed to deal with situations linked to it. As the Managing Director of Kaspersky Lab Asia Pacific, Stephan Neumeier, noted, "Countries like India are developing so quickly, it opens the possibilities for additional cyberattacks."[25]

While technology may be utilized to protect smart cities, it also has the potential to become a security nightmare. When a city's whole infrastructure, including its power plants, water supply, traffic lights, and public transportation, is connected to the internet, there is a significant risk. Although electronic surveillance is intended to make cities safer, there are still weaknesses that might result in inter-communal conflict, growing crime rates, many terrorist attacks, an increase in crimes against women, and societal discontent.

---

[22] Paul Pierce, et al., 'Smart Cities as Organizational Fields: A Framework for Mapping Sustainability-Enabling Configurations' (2017) 9 Sustainability <https://econpapers.repec.org/article/gamjsusta/v_3a9_3ay_3a2017_3ai_3a9_3ap_3a1506-_3ad_3a109605.htm> assessed 20 November 2022

[23] Kim Zetter, 'H(ackers)2 O: Attack on City Water Station Destroys Pump' (*Wired*, 18 November 2011) <https://www.wired.com/2011/11/hackers-destroy-water-pump/> assessed 20 November 2022

[24] Sushma Devi, 'Cyber Security In The National Security Discourse' (2019) 23(2) World Affairs: The Journal of International Issues 146-159

[25] Mugdha Variyar, 'Kaspersky Flags Cyber Threats to Digital India' (*The Economic Times*, 7 July 2017) <https://economictimes.indiatimes.com/small-biz/security-tech/security/kaspersky-flags-cyber-threats-to-digital-india/articleshow/59483374.cms> assessed 20 November 2022

Anand Navani, the country manager for Verint Systems, asserts that technology can play a significant role in enhancing city safety. The efficiency of the entire system in a smart city will be greatly increased by modernizing the police force and giving them access to the newest technologies.[26]

India has seen an upsurge in cyberattacks as a result of hackers becoming more interested in the country's expanding digitalization and economy. For instance, in June 2017, the malware attack "Petya" targeted India's largest container port facility, the Jawaharlal Nehru Port Trust near Mumbai. The attack prevented the terminal from loading or unloading cargo or even from determining which container belonged to whom. The attack revealed both India's cyber infrastructure's vulnerability and the dearth of trained personnel to deal with similar situations.[27] Therefore, it is crucial to have employees with security expertise as well as enough funding, cutting-edge training, and tools to support employees in developing such abilities. It is essential to make sure that the nation has efficient monitoring, secure infrastructure, and a plan of action in event of a cyberattack. For safer cities, all stakeholders—including law enforcement, emergency response systems, and government agencies—must cooperate. Emergency plans must be created, and experts must be trained to address cyber-related risks, in smart cities.

CYBER LAWS IN INDIA

In order to stop crimes committed through computer resources and Internet technology, "Cyber Law" was introduced. "Cyber Laws" can be defined as the legal issues that are related to the utilization of communication technology, concretely "cyberspace", i.e., the Internet. It is an endeavor to integrate the challenges presented by human action on the Internet with a legacy system of laws applicable to the physical world. It is important as it is concerned with almost all aspects of activities and transactions that take place either

[26] 'Are Smart Cities Prepared for Cyber Attacks?' (*Smart Cities Council*, 07 August 2017) <https://www.smartcitiescouncil.com/article/are-smart-cities-prepared-cyber-attacks> assessed 20 November 2022

[27] 'Cyber Security: India's growing Economy, Digital Push put India at Greater Cyber Attack Risk, says Kaspersky Lab' (*Financial Express*, 16 July 2017) <https://www.financialexpress.com/life/technology/cyber-security-indias-growing-economy-digital-push-put-india-at-greater-cyber-attack-risk-says-kaspersky-lab/765231/> assessed 20 November 2022

on the internet or other communication devices. Whether we are aware of it or not, each action in Cyberspace has some legal and cyber legal views[28].

Based on the United Nations Model Law on Electronic Commerce (UNCITRAL), 1996, the Indian Parliament passed the *Information Technology Act, 2000* (also known as IT Act no. 21 of 2000) on 17th October 2000. This law was introduced in India to deal with digital crimes or cybercrimes and electronic commerce.

Some key points of the Information Technology (IT) Act, 2000 are as follows:

- E-mail is now considered a valid and legal form of communication.
- Digital signatures are given legal validity within the Act.
- The Act has given birth to new businesses to companies to issue digital certificates by becoming the Certifying Authorities.
- This Act allows the government to issue notices on the internet through e-governance.
- The communication between the companies or between the company and the government can now be through the internet also.
- Addressing the issue of security is the most important feature of this Act. It introduced the concept of digital signatures that verifies the identity of an individual on the internet.
- In case of any loss or harm done to the company by criminals, the Act provides a remedy in the form of money to the company.[29]

Since the Information Technology Act, 2000 did not cover all the aspects of cybercrimes committed; amendments were done in the Rajya Sabha on 23rd December 2008, renaming the Act as the Information Technology (Amendment) Act, 2008, and was referred to as ITAA, 2008. Eight new Cyber Offences were added to ITAA, 2008 under the following sections:

[28] Nikunj Arora, 'Cyber crime laws in India' (*iPleaders*, 28 April 2022) <https://blog.ipleaders.in/cyber-crime-laws-in-india/> assessed 20 November 2022
[29] ibid

Sr. No.	Sections under the Information Technology (Amendment) Act, 2008	Punishment
1.	**Section 66A:** *Cyber Stalking*, i.e., sending offensive messages through any communication services like a computer or mobile phone	Imprisonment up to 3 years long with a fine.
2.	**Section 66B:** *Receiving stolen computer's resources or communication device dishonestly*	Imprisonment which may extend up to 3 years, or with a fine of rupee 1 lakh or both.
3.	**Section 66C:** *Identity Theft*	Imprisonment which may extend up to 3 years along with a fine that may extend up to rupee 1 lakh.
4.	**Section 66D:** *Phishing*, i.e., punishment for cheating by personation by the use of computer's resources	Imprisonment which may extend up to 3 years along with a fine that may extend up to rupee 1 lakh.
5.	**Section 66E:** *Voyeurism*, i.e. punishment for violating privacy of an individual	Imprisonment for 3 years along with a fine which may be extended up to 2 lakh rupees or both.
6.	**Section 66F:** *Cyber Terrorism*	Life imprisonment.
7.	**Section 67A:** *Publishing/ or transmitting material in electronic form containing sexually explicit contents*	Imprisonment up to 5 years along with a fine that could extend up to 10 lakh rupees in the first convict; and imprisonment can be extended up to 7 years

		with fine of 20 lakh rupees in the second convict.
8.	**Section 67B:** *Child pornography*	Imprisonment up to 5 years along with a fine that could extend up to 10 lakh rupees in the first conviction; and imprisonment can be extended up to 7 years with an extended fine of 10 lakh rupees in the second conviction.

Following are some of the *important Sections under the Indian Penal Code* for the protection of individuals from Cybercrimes:

Sr. No.	Sections under the Indian Penal Code (IPC)	Punishment
1.	**Section 354A** punishes the offense of *Sexual Harassment*	3 years of imprisonment and/or fine.
2.	**Section 354C** criminalizes the offense of *Voyeurism*, i.e., the act of capturing the image of a woman engaging in a private act, and/or disseminating said image, without her consent	3 years of imprisonment for the first conviction and 7 years of imprisonment for the second conviction along with a fine.
3.	**Section 503** punishes *Criminal Intimidation* as threats made to any person with an injury to her reputation	Imprisonment which may extend up to 2 years, and/or fine.

4.	**Section 507** punishes *Criminal Intimidation* by an anonymous communication	Imprisonment may extend up to two years.
5.	**Section 228A** deals with the *vengeful posting of images or videos of rape victims*	Imprisonment which may extend up to two years and a fine.

Apart from the above-mentioned Sections under the IPC and ITAA, 2008, the Government of India has taken the following steps for the prevention of Cybercrimes:

- *Cybercrime cells* have been set up in states and U.Ts for reporting and investigation of Cybercrime cases.
- The Government under the IT Act, 2000 has also set up *Cyber Forensic and Training Labs* in the states of Kerala, Assam, Mumbai, Mizoram, Manipur, Nagaland, Arunachal Pradesh, etc., for awareness creation and training against Cybercrimes.
- In collaboration with the Data Security Council of India (DSCI), and NASSCOM, *Cyber Forensic Labs* have been set up in Mumbai, Bengaluru, Pune, and Kolkata for awareness creation and training.
- Various programs have been conducted by the Government of India to generate awareness about Cybercrimes. *National Law School, Bengaluru,* and *NALSAR University of Law, Hyderabad* are engaged in conducting several awareness and training programs on Cyber Laws and Cybercrimes for Judicial officers.
- Training is imparted to Police officers and Judicial officers in the *Training Labs* established by the Government.[30]

PAKISTAN

It is estimated that the annual cost of cybercrime will roughly increase from 3$ TD (Trillion Dollars) in 2015 to 6$ in 2021. In 2015, the market for cyber security products and services spent $75 billion dollars. This amount increased to a record-breaking $101 billion in 2018, and it is predicted that this amount will reach $170 billion dollars in 2020.

[30] ibid

The European nations created the EGDPR (European General Data Protection Regulations) and the Second Directive, which are used to secure the information in systems from threats (Network Information Security). It is a strategic battle for Pakistan's survival that the country is currently focusing on at a time when the Pakistani army is under threat from terrorists as well as from Chinese and Indian cyber security concerns.[31]

Pakistan is engaged in two conflicts: one with terrorists, and the other with concerns about cyber security. Since 1990, Pakistan has had access to the internet. In 2018, there were 200,813,818 people living in Pakistan, or 2.97% of the world's population. Pakistan is ranked sixth in terms of population, with a density of 250 people per square kilometer and a 39.6% urban population. With a population of 200,813,818 people, Pakistan has 44,3424 million internet users. In addition, there are 1 million new mobile members each month. Roughly 16.5 million of these users browse and use the internet on their mobile devices, while the rest are broadband customers. 80% of smartphones were found in Pakistan for less than $100.[32]

Information and communication technology is Pakistan's fastest-growing industry. According to an ITU (International Telecommunication Union) survey, 20 million people used the internet at the end of 2012, up from an estimated 6.7% of the population in 2006 and an estimated 1.3% of the population in 2001. ISPAK (Internet Service Provider Association of Pakistan) stated that the number is approximately 10 million as of 2012. In addition to these reports according to IT THINK TAMKS, the number should exceed 30 million. Pakistan will have 3G and 4G starting on April 14, 2014. The amount the Pakistani government received from the 3G and 4G auctions were $930 million and $210 million, respectively. 50 million cellular subscribers, 56 million 3G/4G subscribers, 3 million basic telephone subscribers, and 58 million broadband subscribers are reported in the PTA (Pakistan Telecommunication Authority) annual report for 2018.[33]

[31] Qamar Atta Ul Haq, Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan (2019) 11(1) IJCNIS 62-69 <https://www.mecs-press.org/ijcnis/ijcnis-v11-n1/IJCNIS-V11-N1-6.pdf> assessed 20 November 2022
[32] ibid
[33] ibid

CYBER CRIMES IN PAKISTAN

Due to a cyber-attack in November 2018, 624 customers from 22 different banks lost 11.7 million in total. According to a legal complaint from the FIA, 19,865 ATM cards' data were sold on the dark web. the practice of leveraging networks and computers to further illegal criminal conduct Cybercrime poses the greatest threat to Pakistan, but unhappily, it is said that the country's laws are inactive and awaiting implementation. 2012 saw the eighth ICT exposition, CONNECT exhibition in Karachi, and reports of almost 200 hacking and extortion instances.

Global researchers on the topic to arrive at and contribute to their experiences significantly include ICANN, APNIC, Internet social club, Google, regional CERTs, and ICANN. The main goal of this conference is to raise awareness of cybercrime and cyberterrorism among Pakistanis. To that end, Cyber Invulnerable Pakistan includes a series of training sessions, workplaces, cognizance sessions, contestants, keynote speeches, panel discussions, and security discussions by eminent internal and external industry experts. Proficient awareness sittings and holding the succeeding training sittings, CHFI (Computer Hacking Forensic Investigation), mobile diligence incursion testing, contrary engineering malevolent program, Linux origin instruments workplace by Pakistan, system protection workplace through ICANN and APNIC. LEA workplace in Pakistan, kid security through the internet society.[34]

In Pakistan, cybercrime is on the rise swiftly. According to the cyber-crime wing (CCU), a division of the FIA Federal Investigation Agency, only events exclusively are reportable to the unit; in 2007, 62 cybercrime-related events were reported to the CCU; in 2008, the number of events quickly increased to 287; and after the passage of laws from the Pakistani parliament, the ratio of cybercrimes declined from 117 events in 2009 to 73 events in 2010. Later, the ratio grows once more and quickly from the previous and preceding ratio of events, which is 2011 to 2012 - 411 incidents, 2013 - 290, 2014 - 320

[34] Qamar Atta Ul Haq, Cyber Security and Analysis of Cyber-Crime Laws to Restrict Cyber Crime in Pakistan (2019) 11(1) IJCNIS 62-69 <https://www.mecs-press.org/ijcnis/ijcnis-v11-n1/IJCNIS-V11-N1-6.pdf> assessed 20 November 2022

with slight blackmailing, 2015 being roughly 345, and beginning in 2016 being 89 events up until March being reported to FIA.[35]

Cyber laws or the inferior conversationally and national laws of Pakistan a consideration that capsulate the effectual consequences associated with the manipulation and the use of communicatory, relations and the disseminative expressions of electronic network entropy gimmicks or devices and engineering. The following Pakistan cyber laws for criminals. 1. ETA The Electronic Transaction Act (1996). 2. ETO The Electronic Transaction Ordinance (2002) 3. PACCA Perspective analysis of Cyber-crime act (2006) 4. EFTA The Electronic Funds Transfer Act (2007) 5. PECOP The Prevention of Electronic Crime Ordinance Pakistan (2007) 6. PECOA Prevention of Electronic Crime Ordinance Act (2008) 7. PCCCOA Prevention and Control Cyber Crime Ordinance act (2009) 8. FTOA The Fair and Trial Ordinance Act (2012) 9. PECOA Prevention of E Crimes ordinance Act (2013) 10. PPOA Protection of Pakistan Ordinance Act (2014) 11. EDPCCOA The Electronic Documents and Prevention of Cyber Crime Ordinance Act (2014) 12. PECOA Prevention of Electronic Crimes Ordinance Act (2015) 13. AECOA Amendment Electronic Crimes Ordinance Act (2016).[36]

SRILANKA

The Sri Lankan Computer Emergency Readiness Team and the Sri Lankan Police's Cybercrime Unit have received several reports of cybercrimes occurring in Sri Lanka. Records kept by the Sri Lankan police indicate that the normal crime rate has reduced. However, the study examines cybercrime. Crimes of this nature have steadily escalated. The Sri Lankan Computer Emergency Readiness Team received reports of cases involving intellectual property, phishing, privacy violations, malware, email harassment, and phony Facebook accounts. Additionally, cybercrime crimes involving e-banking, website hacking, email harassment, and child pornography have been reported to the Sri Lankan police's cybercrime unit.[37] The majority of the cases involved phony Facebook accounts.

[35] ibid
[36] Rashida Zahoor & Naseem Razi, 'Cyber-Crimes and Cyber Laws of Pakistan: An Overview' (2020) 2(2) PRJAH 133-143
[37] A H Dinithi Jayasekara, 'Internet and law (special reference to Sri Lanka)' (2015) 10(6) The Social Sciences 841-844

Defamation, however, is treated as a civil matter rather than a criminal offense in Sri Lankan law. There are four primary acts that have been employed in Sri Lanka to prevent cybercrime. The Computer Crime Act of 1997 was quite significant. No definition of cybercrime is provided in this act; nonetheless, the phrase "computer crime" is used to refer to all crimes and fraud involving computers and information technology. This law can be broken down into two sections and it covers a wide variety of offenses. They were hacking offenses and computer-related crimes.[38]

An offense includes securing unauthorized access to a computer, taking any action to do so in order to commit an offense, causing a computer to execute a function without legal authorization, and offenses against public order, national security, and the economy. Additionally, interacting with illicit data is illegal as is illegal data acquisition, illegal data interception, illegal device use, and illegal disclosing information to gain access to a service. The scope of the intellectual property laws in the Intellectual Property Act 36 of 2003 is expanded by a clause of the act. A 2006 modification to the penal law created an offence requiring anyone offering computer services, such as those offered at cyber cafés, to ensure that those services won't be used for crimes involving the sexual abuse of children.[39]

Additionally, information technology, communication, and related acts and the electronic transactions act particularly address crimes committed online. The creation and sharing of data communications, electronic documents, and electronic records are all made easier under the Electronic Transaction Act. Additionally, these offenses are avoided by using the Penal Code Amendment and Evidence (Special Provisions) Act (No. 14 of 1995). Penal Code Amendment: The "Duty of Person Providing Service via Computer to Prevent Sexual Abuse of a Child" provision is found in Penal Code Amendment 286(b). These measures support safeguarding kids from unauthorized internet. To help Sri Lanka create cyber security regulations, efforts have been made to write the Defense Cyber Commands Act and a bill imposing cyber protection rules. The suggestions presented by the President

[38] A. H. Dinithi Jayasekara & Wijayananda Rupasinghe, 'Cyber-Crime in Sri Lanka' (2015) 12(10) Journal of US-China Public Administration 759-763
[39] ibid

in his capacities as Minister of Defense and Minister of Technology have received approval from Cabinet.[40]

BANGLADESH

To prevent unwanted cyber incidents using telecommunications tools, Bangladesh passed the Telecommunication Regulation Act in 2001. Since social media had not yet been created or made public at the time, the Act did not address cybercrime committed through these platforms, but it did make it clear that crimes committed online via telecommunications would be subject to legal sanctions.

Early in 2006, Bangladesh enacted the Information and Communication Technology Act (hereafter referred to as the "ICT Act 2006") as a forceful response to cybercrimes. The Act enables law enforcement organizations to look into an offense and prosecute the criminal before the Cyber Tribunal. The ICT Act of 2006 in question was amended in 2013 by the government of Bangladesh, which altered the way in which online offenses were prosecuted under the Act's penal provisions. The National Cyber Security Strategy of Bangladesh 2014 (hence referred to as the "NCSS 2014") and the Information Security Guidelines 2014 were created by the ICT Division the following year.[41]

The NCSS exclusively addresses the nation's national security policy, and its goal is to develop a cogent vision for 2021 that will keep Bangladesh safe and wealthy by coordinating efforts on both a domestic and international level to defend cyberspace. The ICT Act and NCSS, however, proved to be insufficient due to the passage of time and the quick growth of cybercrimes. In the meantime, social media captured the attention of the general public, and daily usage increased. As a result, the government passed the Digital Security Act 2018 to combat the unprecedented cybercrimes carried out online.

The Digital Security Act addresses a wide range of recent cybercrimes, including offenses involving unauthorized access to critical information infrastructure, the dissemination of

[40] 'Formulation of laws on cybersecurity in Sri Lanka' (*Lanka Express*, 12 October 2021) <https://www.lankaxpress.com/cyber-security-laws-in-sri-lanka/#:~:text=Cyber%20Security%20Laws%20in%20Sri%20Lanka%20Sri%20Lanka,Minister%20of%20Defense%20and%20the%20Minister%20of%20Technology.> assessed 20 November 2022

[41] Md Abu Bakar Siddik & Saida Talukder Rahi, Cybercrime in Social Media and Analysis of Existing Legal Framework: Bangladesh in Context (2019) 5(1) BiLD Law Journal 68-92 <https://bildbd.com/index.php/blj/article/view/34/32> assessed 20 November 2022

disparaging information, tampering with computer source code, digital or electronic fraud, etc. The Act includes penalties for online publication of objectionable material, cyberterrorism, defamation, and other offenses, but it excludes social media-related criminality from its scope. The current legal framework must be examined to determine whether the rules are sufficient to combat cybercrimes committed using social media in order to remove any legal obstacles.

A unique body known as the Cyber Tribunal was also established by the amendment to hear cases under the ICT Act. In an effort to boost the percentage of convictions, the Tribunal was established with strict rules regarding the amount of time it had to resolve cases. A relatively small number of cases were actually brought before the Tribunal's courts within the first few years after its founding. There were fewer than 200 cases submitted to the Tribunal in the first three years of its existence. There have also been issues with the speed at which cases have been resolved; according to reports, the Tribunal's conviction rate was 3% up until 2019.[42]

NEPAL

Cyber law is the body of law that addresses a variety of issues related to the internet and other forms of communication technology, as well as the rights and jurisdictions that govern cyberspace. The Electronic Transaction Act (ETA) 2063, passed in 2004, is known as cyber law in Nepal. Cyber law is the body of law that regulates events that take place in the immaterial digital world, such as providing immaterial information in cyberspace with legal standing. Cyber laws are essential and effective for managing cyber issues.[43]

The government must be open and honest in how it operates. The State is responsible for enacting tough enough laws to deter cybercrime, deter potential offenders, attract them, and put an end to the abuse of the Internet and other cybermedia for any criminal actions. The primary goal of security is to protect an organization's ICT resources. Assets like

[42] ibid

[43] Shailendra Giri, Cyber Crime, Cyber threat, Cyber Security Strategies and Cyber Law in Nepal (2019) 9(3) Pramana Research Journal 662-672 <https://www.researchgate.net/profile/Shailendra-Giri-3/publication/338986738_Cyber_Crime_Cyber_threat_Cyber_Security_Strategies_and_Cyber_Law_in_Nepal/links/5e36ebc392851c7f7f17a07d/Cyber-Crime-Cyber-threat-Cyber-Security-Strategies-and-Cyber-Law-in-Nepal.pdf> assessed 20 November 2022

data, information, knowledge resources, software, hardware, and networks, among others, could be internal or external.[44]

The threat posed by cyber warfare to highly digitized societies and cultures is significant. No nation has been able to create a security strategy that completely ensures the security of communication procedures globally. For a variety of activities, including service delivery and procurement, regulatory adjustments are necessary. The organizations in charge of enforcing cyber laws vary greatly between nations.[45]

AFGHANISTAN

After the interim government was established in late 2001, Afghanistan entered new eras of political and socioeconomic rehabilitation and reconstruction. The ensuing transitional and elected Afghan governments enacted new laws that encouraged private businesses to invest in the nation and offer a range of services to the Afghan people, including telecommunications and ICT. Among the sectoral government bodies in Afghanistan, the Ministry of Communications and Information Technology (MCIT) was the first to develop new strategies and policies that allowed the private sector to make sizable investments in the telecommunication and IT sectors.[46]

The first Cyber Emergency Response Team (CERT) in Afghanistan was founded by MCIT in 2009, and it was given the acronym AFCERT. The goal of AFCERT was to combat cyber threats and crimes while educating the public and private sectors about cybersecurity issues and offering them remedies. In its first two years of existence, AFCERT officially reported an increase in cyber and electronic crimes in the nation to the MCIT high management. It was crucial to carry out a risk assessment of all government ICT infrastructures and develop a strategy to reduce those risks in order to combat the aforementioned crimes. The MCIT and ICT Council approved AFCERT's

[44] ibid
[45] ibid
[46] ZMARIALAI WAFA, 'National Cyber Security Strategy of Afghanistan (NCSA)' (*ITU-IMPACT*, November 2014) <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Afghanistan_2014_National%20Cybersecurity%20Strategy%20of%20Afghanistan%20(November2014).pdf> assessed 20 November 2022

request to prepare a national cyber security strategy, and for that purpose, the MCIT and ICT Council formed a committee.[47]

The inaugural NCSA awareness training was held in 2012 at the ICTI Institute with support and funding from the US Department of Commerce. All government CIOs, ICT directors, business executives, and academics attended the four-day event to learn about and analyze diverse international strategies. The Information Systems Security Directorate of MCIT served as the NCSA committee's chair, and it held regular meetings and evaluations for a full calendar year. The NCSA committee completed and submitted the initial draught of the strategy to the MCIT and ICT Council in July 2014 for review and adaptation of its action plan following a series of evaluations and recommendations.[48]

CONCLUSION

Online fraud can sometimes be highly effective and persuasive. The troublesome aspect of these frauds is that their perpetrators are quite difficult to identify, which contributes to their daily growth. According to the research mentioned above, India is ranked third in the world for the frequency of cybercrimes. India currently has cyber cells in every province, however, many people were not aware of their presence. Therefore, better technology and networking systems must be designed and implemented for securing people's vital data in order to reduce cybercrimes.

In addition, awareness workshops must be held to educate people about the many forms of cybercrimes and the security measures that may be put in place to protect their data, especially women, children, and senior citizens. It is possible to raise awareness of cybercrimes with 3D animation teaching methods. Without a global commitment that is taken seriously, it is almost impossible to entirely eradicate cybercrime. To make use of the advantages of the digital age, we must protect ourselves from cybercrimes and be extremely vigilant and knowledgeable about the most recent scamming techniques.

There aren't enough laws in Pakistan to safeguard people's, organizations', societies', and states' online rights. Therefore, it is imperative to deal ruthlessly with this cyber monster, also known as cybercrime. Such laws may be created to punish offenders in a

[47] ibid
[48] ibid

way that serves as a deterrent. Additionally, the Pakistan Penal Statute, 1860 might be updated to incorporate cybercrimes within the current code. Additionally, specific cyber laws may be passed to safeguard the institutions. This will support the institutions' efforts to safeguard consumer information and increase customer confidence. Similarly, by creating an appropriate security plan and policy, sensitive information regarding the security of the state may also be protected. A group of experts should be assembled to manage, safeguard, and look into societal, institutional, and individual cyber issues.

Afghanistan is seeing a similar outcome as a result of cyberterrorism. There is an urgent need for new laws to close the gaps and stop cybercrimes and cyberterrorism. Due to redundant provisions in numerous statutes, Bangladesh's current laws are comprehensive but technically risky and complex. Therefore, a specific regulation is required to control cybercrime on social media. Many foreign nations are considering enacting this kind of regulation, and others have actually taken action. No country is immune to the threat of cybercrime, including Nepal. Cybercrime is being nurtured by rising internet and computer usage as well as technological advancement. Because of its insufficient laws and regulations, Nepal confronts significant obstacles. The number of cybercrimes is increasing daily, and people, businesses, and governments are finding it difficult to protect themselves. Since IT is transforming every element of human behavior, cyber law is now crucial.