Library Progress International *Print version ISSN 0970 1052*
Vol.44 No.3, Jul-Dec 2024: P.4618-4627 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Examining the Role of Cyber-Security in Combating Economic Repercussions of Cyber-Crimes: Strategy for India

Shraddha Shukla[1], Ravi Kant[2], Dr. Charu Srivastava[3], Aman Gautam[4], Dr. Pratishtha Yadav[5]

[1]Research Scholar, School of Law, Christ University (Delhi-NCR).
[2]Assistant Professor, ICFAI University, Hyderabad.
[3]Associate Professor, School of Law, UPES, Dehradun.
[4]Research Scholar, School of Law, Sharda University, Greater Noida, UP.
[5]Assistant Professor, Alliance School of Law, Alliance University, Bangalore.

How to cite this article: Shraddha Shukla, Ravi Kant, Charu Srivastava, Aman Gautam, Pratishtha Yadav (2024). Examining the Role of Cyber-Security in Combating Economic Repercussions of Cyber-Crimes: Strategy for India. *Library Progress International,* 44(3), 4618-4627.

ABSTRACT

The internet penetration level for India has taken a steep rise in the recent past. Not only metropolitan cities but also towns and villages are witnessing the ease of internet availability. Although cyberspace provides ease and convenience in many aspects, it also brings in certain drawbacks and concerns for the users. These concerns are largely related to the protection of data on the internet. The research article begins with an introduction which summarizes the theme of the research, followed by a review of literature to explore different issues, and gaps in the area of research. The authors have used library-based doctrinal research methodology relying upon secondary data sources to explore, describe, analyze, and discuss the economic repercussions of digital crimes. The research on each section of this article has been done in consonance with the development of policies in India. Our findings conclude that creating a cyber-resilient environment along with a collaborative legal framework to address cybercrimes would help the nations in securing their economy from cybercrimes. India must fast-track the implementation of its National Cyber Security Strategy and work on establishing exclusive courts for resolving cyber security matters.

Keywords: Cyberspace, economy, digital crimes, cyber-resilience, cyber-security.

"If you think you know-it-all about cybersecurity, this discipline was probably ill-explained to you."
— Stephane Nappo

1. Introduction

Sir William Blackstone (1769) while writing the Commentaries on the Laws of England defined the term 'crime'. He said that violation of any right of an individual by another is called a crime (Blackstone, 1769, p. 5). It has always been a part of society since the very inception of human civilization. Emile Durkheim said "to think of a crime-free society is a myth" (A. Sharma & Krishna Pallavi, 2017).

Cyber Crime is relatively a new concept of crime that emerged because of Computers and the Internet. These crimes are on an exponential rise since their inception. Every year a new type of cybercrime occurs which is unknown to society. So, it becomes difficult to predict to what extent it will harm different aspects of society like its effect on human values, culture, beliefs, youth, finance, management, global economy, businesses, etc. Human values are questioned by the commission of new cybercrimes, they tend to shake the cultural beliefs. Businesses lose a lot of their wealth on preventing or curing the harms caused by cybercrime attacks on their organization. In the year 2018, a Pune-based Cosmos Bank lost Rs. 94.42 Cr/- when hackers siphoned off this amount by gaining a backdoor entry into the bank's ATM server (Kratikal, 2019). In the same year, Canara Bank also lost Rs. 20

lakhs/- when hackers used a skimming device to stole cardholders' details and further transferred this whole amount in small transactions varying from Rs.10,000/- to Rs. 40,000/-. After the Aadhaar Software of UIDAI was hacked wherein the personal data of around 1.1 billion users was compromised, the Central Government issued a caution for all the Aadhaar holders to not share a copy of their Aadhaar Card with any organization without verifying their valid license. Only those organizations can seek a copy of the Aadhaar card for establishing the identity of a person who has obtained a User License from the UIDAI (Department of Land Resources, 2022).

All these attacks on businesses and organizations lead to the loss of economic value of the country. The economic growth of the country is hampered and slowed down because of the massive monetary loss. Few small businesses who experience a cyber-attack may sometimes never recover, for others, it creates a hardship in running or resuming their business transactions. COVID-19 lockdown induced cyberattacks which increased the amount of debt on the economy of businesses and further created a negative impact on the economic growth of the country. Fraudsters have been implementing state-of-the-art technology to defraud the gullible people of their hard-earned money.

To reduce its impact, it is crucial to adopt the best cyber security practices. However, the first and foremost thing is to create awareness among the general masses. CERT-In, RBI, MeitY, Cyber Peace Foundation, and several other organizations are working at the ground level to spread awareness regarding cybercrimes and cyber security measures. The elementary caution is that no one should ever share their sensitive personal information, especially the financial information. It must always be kept confidential and secure. RBI has published a booklet that emphasizes on practicing due diligence while performing a financial transaction anywhere (Reserve Bank of India, 2022). "Be Aware and Beware!" is the theme of this booklet.

For any fraud to be committed on financial transactions, the weakest link is the end-user. It is important for the user to take great precautions while transacting money. The user must be cautious of any suspicious pop-ups on the internet. The payment must be made through a secured payment gateway, i.e., https:// shall be present in the URL along with the lock symbol. Sensitive personal information like ATM PINs, passwords, CVV, and Card numbers must never be shared with anyone including financial institutions, family, and friends. The 2FA facility shall be availed wherever it is available. E-mails or messages originating from unknown sources shall not be responded to and replied to. Any suspicious attachment along with the message shall be deleted without opening it. The copy of the cheque book and KYC documents shall not be shared with a stranger. The use of virtual keyboards should be increased when entering a password on banking websites. The passwords shall be changed periodically and no two websites or accounts shall have the same string of passwords.

With the growing use of IoT devices and cloud-based services, it is inevitable for a user to stay offline. Internet connectivity is the sole platform on which these services and devices work. And all-time connectivity results in increased vulnerability to cyber-attacks. India saw a 22% increase in attacks on IoT devices, according to a report by Indian digital services firm Subex (News18, 2019). This is the second time that India has topped the number of cyber-attack victims. It becomes crucial for a developing country like India to have strong legislation backed up with the latest technologies like Blockchain, AI, Drone, etc. These cutting-edge technologies have immense potential to be explored and utilized in the better management and security of financial transactions. A permissioned Blockchain may be started by RBI wherein all Indian Banks can act as validators for all transactions within India. AI can also be used for better analysis and prediction of future difficulties. In this way the impact of modern financial crimes on the economy can be minimized with the use of technology.

Literature Review

In the year 2017, World Economic Forum (WEF) suggested that an increasing dependency of the global population upon cyberspace would also increase the plausibility of cyber-attacks in the world (Forum, 2017). Recent times have already witnessed that there is a record-breaking increase in the use of technology across nations. The apparent cause has been the worldwide pandemic. As a consequence of which people had to adapt to technological means for carrying out their work and communicating with each other. The internet service saw a rise of 100% from a 40% pre-lockdown phase (De' et al., 2020). Many services, for instance, education, commerce, entertainment, and health had to be made accessible via the internet so that citizens do not have to violate the social distancing norm. But with comfort, also came the downside of the same. Depression, anxiety, loneliness, online gaming addiction, poor sleep quality, loneliness, and escapism were frequently reported symptoms among adolescents (Fernandes et. al., 2020).

The growth of cyberspace has been a dynamic process with respect to its scale, speed, data creation, number of users, and interconnectivity. As a result of this, machines have become more intelligent. It is believed that in the coming future the entire system will be so complex and sophisticated that we as humans might end up becoming mere observers of it (Sadie et al., 2020). Such advanced information technology domain has put forth a shortage of technologically skilled employees, especially in the cyber-security field (Teoh & Mahmood, 2018). It is pertinent to note that there has been a steep rise in the graph of cyber-attacks vis-à-vis progression toward cybersecurity measures (Sviatun et al., 2021). These cyber-attacks or cyber-threats have shown a 358% increase in the recent past (Higbee et al., 2022). In India also, according to the data from National Crime Records Bureau (NCRB), there has been a rapid increase in the number of cybercrimes (National Crime Records Bureau, 2015, 2016, 2017, 2018, 2019, 2020) (see Fig. 1).

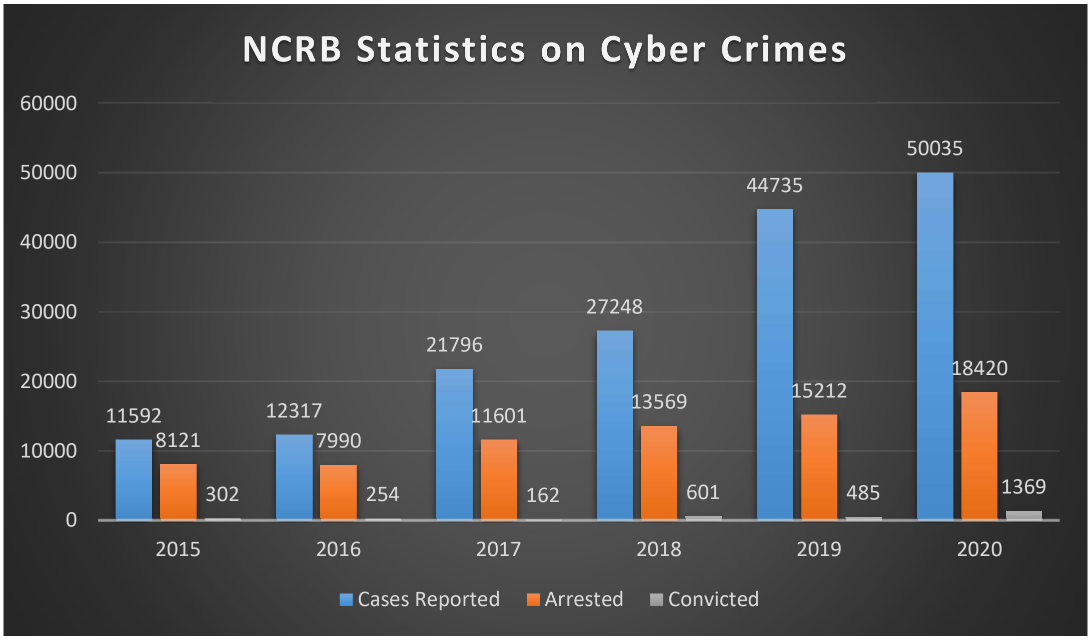


Fig. 1 Increasing rate of cyber-crimes in India and the gap in conviction rate. Source Drawn by authors from NCRB (2020)

Cyber-crimes like traditional physical-world crimes are also committed with a motive. This statement can be best explained by the Rational Choice Theory given by Cornish and Clarke, which is based on a utilitarian belief that every action of a man is influenced by a rational choice (Rajput, 2020, p. 28). This choice is implemented only by weighing the means and ends of doing it and the related costs and benefits attached to it. The motive behind a cyber-crime can either be a personal benefit or a monetary benefit (Kshetri, 2013). A sub-theory of Rational Choice Theory is the Routine Activity Theory which is a creation of Marcus Felson and Lawrence Cohen. According to this sub-theory if the target is not well protected and there are substantial benefits attached to it then the probability of a crime being committed against that target is high. (Rajput, 2020, p. 29) A target is more vulnerable when it uses information technology for carrying out its business and has a huge financial turnover (Sviatun et al., 2021).

Committing an economic crime in cyberspace is a sub-category within cyber-crimes. This type of cyber-crime has a motive to attain monetary benefits from the target or victim. The target can either be an individual, an organization/firm, or a country's government. Based on the gravity of a cyber-crime and the repercussions it entails, the legislature decides the severity of the punishment for such a crime in a society. In today's times, ransomware gangs are not just encrypting and stealing information, but they are also leaking sensitive data to put added pressure on the victims. The primary motive to do so is to extract a huge pay-out from the victim (O'Murchu, 2022). It had been proposed that the damage caused by cybercrimes would cost around $6 trillion per year by 2021 (Prakash & Singh, 2021). In 2017, ransomwares like WannaCry, Petya and EternalBlue demanded the ransom in bitcoins (Forum, 2017), which is (Bitcoin) altogether another technological breakthrough in the contemporary world. Its creation has revolutionized the global economy by breaking down the traditional rules of currency and subsequently developing a universal digital economy (Teoh & Mahmood, 2018).

India's economy is rising gradually and it has been proposed that in the next decade it will be the third-largest economy in the world (Mint, 2021; Y. S. Sharma, 2022). As a result of which it might attract ransomware attackers to extract large pay-outs. The growing cyber-threats in every aspect of our lives have created a huge demand for a cyber-security workforce (Teoh & Mahmood, 2018) and cyber security countermeasures. The Information and Technology Act, 2000 (IT Act) of India defines "cyber security" under S. 2(1)(nb) as a method used for protecting information, electronic communication channels, and computer network systems from unauthorized access, misuse, and destruction. The Central Government of India has been empowered under S.16 of the IT Act to prescribe rules and regulations for security procedures (The Information Technology (Security Procedure) Rules, 2004). These procedures and practices are to be complied with while securing an electronic record or an electronic signature. Another initiative of the Indian Government towards cyber security is the establishment of its Computer Emergency Response Team (CERT-In) which is an organization under Ministry of Electronics & Information Technology. CERT-In reported a 121% increase in the cyber-threats incidents from 2020 to 2021 (Indian Computer Emergency Response Team, 2022).

An international approach to provide a comprehensive law for cyber-crimes and cyber operations has been attempted by Schmitt & Vihul in their manual on "Tallinn manual 2.0 on the international law applicable to cyber operations" (Rajput, 2020, p. 39). Amongst other counter measures, blockchain technology is being implemented for securing critical information in sectors, like finance, certificate records, health records, etc. (Upadhyay, 2020). In addition to that, operational cooperation amongst countries is the need of the hour to combat cyber related attacks and crimes (Sviatun et al., 2021). The European Union (EU) has already come up with a proposal for regulating the risk management of financial institutions using a unified framework known as Digital Operational Resilience Act (DORA). This proposal would establish uniformity across European Union member nations for regulating the cyber security and governance of financial service providers (Chantzos, 2022). World Economic Forum's Centre for Cybersecurity is another collaborative action toward bridging the gap between cyber security experts and the government bodies to take decisions in light of a cyber-resilient policy (World Economic Forum, 2020). In light of the National Cyber Security Policy 2013, the Government of India established a National Cyber Coordination Centre to coordinate amongst the national cyber-security and surveillance agencies and generate real-time data on cyberspace vulnerabilities (Press Information Bureau, 2018) and also to coordinate with other nations in cybersecurity risk management. Recently, CERT-In has entered into a bilateral agreement with Japan and Nigeria to coordinate on cybersecurity issues and on information sharing with respect to resolving cyberspace incidents (Indian Computer Emergency Response Team, 2022).

According to Ken Xie who is the Founder, Chairman, and CEO of Fortinet - "There must now be a different approach to cybersecurity. Our current approach is unsustainable." (Bissell & Pipikaite, 2022). It implies that the nations should now focus on moving from cyber security to cyber resilience. Cyber resilience is an umbrella term which encompasses the ability of an organisation to dodge a cyber-attack, protect its critical infrastructure, maintain continuity in the business and other processes, and secure information (De Groot, 2019). Cyber resilience is the most apt solution to cyber-attacks in today's times as it works on the principles of - threat protection through technologically advanced and sophisticated tools, the ability to recover data in cases of ransomware attacks, adaptability of the organization to detect an attack and respond to it quickly, and durability of the organization to function normally after an attack. If the cyber-policy of a company works on making it more cyber-resilient then the overall business infrastructure of an organization would become more durable in securing the finances as well as critical information.

2. Evolution of Advanced Crimes

In the modern age, society has progressed a lot in terms of culture, art, social development, science, etc., (Khanna, 2021). The field of science and technology has seen exponential growth, especially due to the introduction of computers in the last century. The evolution of the Internet in the late 1980s changed the way societies interact. It had also fundamentally altered the nature and scope of crimes. The birth of cybercrime happened because of the rapid adaptation of the Internet by the masses. The word cybercrime means and includes all criminal activities that are done with the assistant of a computer device or which harms a computer device or computer network (Dennis, 2019).

In 1990s the advancement in web browsers led to a wave of new viruses which were circulated via Internet. The end users were at very high risk due to the vulnerability caused by dubious websites. Trojan-horse, Email

Spamming, Worm attack, etc., were prominent tools to commit crime on computer resource. The attackers at that time had prominently three motives: Curiosity; Money; Political gains (Dieselcafe, 2014).

With the premiere of social media in the early 2000s, the cybercrime grew unparalleled. Every individual on social media was publishing his personal information which was “a box full of jewels” for hackers to steal. Different criminals used this information and committed financial crimes by creating fake bank accounts and setting up bogus credit cards (Acharjee, 2021). The radical change and shift towards the information era led to an ease of committing crimes like Identity Theft, Cyber-Extortion, Phishing and Vishing, Cyber-Terrorism, Hacking, Online Defamation, Harassment, Unlawful access of Computer, DDoS attack, Salami attack, Web Jacking, Cyber-Stalking, Intellectual Property Theft; Exploitation of children, etc.

3. Crimes of 21st Century

To begin with, we all must keep in mind the famous saying of Stephane Nappo, “One of the main cyber-risks is to think they don’t exist. The other is to try to treat all potential risks” (Nappo, 2019).

The modern *economic crimes* have their roots in telecommunication. Phishing is the easiest and most convenient methods of committing economic crime in digital age. A method in which a user is tricked to give his sensitive personal data willingly is known as Phishing (Acharjee, 2021). In the very beginning it used a worm e.g., ILOVEYOU which was downloaded on victim’s computer for committing the attack. But now a days it has become quite sophisticated that a user won’t get to know of any existence of a worm in his computer. The phishing email also looks to be originating from a trustworthy source.

In the recent years, due to increase in the Internet traffic, the threats of Ransomware have been on rise. The increasing importance of data have led to the growth of ransomware crimes. The documents of any business network are so crucial that a single attack by ransomware could make the attackers earn hundreds of thousands or even millions of rupees. Attackers are always a step ahead, if the business owner doesn’t pay the money, then the attackers threat them that they will reveal the secret documents of the business out in the public. These techniques are employed by attackers to make their demands (extortion) fulfil quickly. The latest trend is to seek money in form of cryptocurrency.

Another type of financial fraud is cryptojacking. Similar to the mining process of cryptocurrency, a cryptojacking is the mining unethically for malicious purpose. Cybercriminals use the devices of other users, after compromising them via a software, to mine the currency.(Acharjee, 2021) This process utilizes the power and energy of victim’s machine to mine or steal money from other’s accounts. Hacker creates a collection of compromised systems (aka Botnets) for speeding the mining process. They siphon the currency into their personal digital wallet via these botnets. Victim’s system uses more CPU power towards mining and this leads to slowing down the machine eventually making it unusable for the victim.

Banking Fraud is the umbrella term which covers all the financial crimes like forgery, fraudulent loans, bank impersonation, ATM Skimming, etc. These crimes are committed via different methods viz by performing a Phishing or Vishing attack; by using some online sales platform; by the use of unverified mobile applications; Card Skimming at POS Service; by the use of screen sharing app or remote access; impersonation through social media; or by SIM swap/cloning (Kulkarni, 2022).

Spoofing a website means creating a hoax website only for the purpose of committing fraud and stealing money. The attackers use the identical name, logo, graphics, source code as of an authentic website to deceive the end user. The sophisticated attackers even create fake URL resembling the real URL of authentic website (Karamchand Gandhi, 2012). The webpages of different payment gateways are spoofed and when a user lands on this payment page, makes a (legitimate) payment but the money is transferred from his account to attacker’s account.

Skimming is another technique where the digital information from a card is copied through the magnetic strip. The copied data is further duplicated on another dumb card which is used for transacting money. Fraudsters use this skimming device to collect the information from credit/debit/ATM cards. The device is attached over the card slot of ATM or merchant payment terminals where the frequency of card swiping is more i.e., where there are large number of transactions occurring. Restaurants, shopping malls, petrol pumps, etc., are the hotspots for this type of crime (Dewi & Septiwidiantari, 2021). Apart from skimming device, a small hidden camera is also positioned in such a way so as to capture the PIN.

As we know there is a requirement of OTP for online banking transactions which is received on the registered mobile number of users. This requirement is also bypassed by the technique known as SIM swap/exchange. Here fraudster manages to get a new SIM for the registered number. Upon activation of the new SIM card, he gets access to all the OTPs and alerts.

Wire Transfer Fraud is another type of financial crime involving wire transfer or the internet (Hurley, 2020). Here the scammers first steal the login credentials like username and password of the banking customer, then they wire money from his account to themselves. It is done via network of interbank fund transfer system because transaction once done is difficult or impossible to reverse (Abrigo, 2013). This mode of transaction is used because of the fact that it is used by banks to settle their accounts with each other and it is commonplace for transacting large amount of money rapidly.

For the general awareness of the masses regarding the digital payments-related frauds, the Reserve Bank of India has published a booklet which illustrates different mode which are used by scammers to commit crime (Reserve Bank of India, 2022). The book also lists few safeguards which the end user must take into consideration while making a financial transaction.

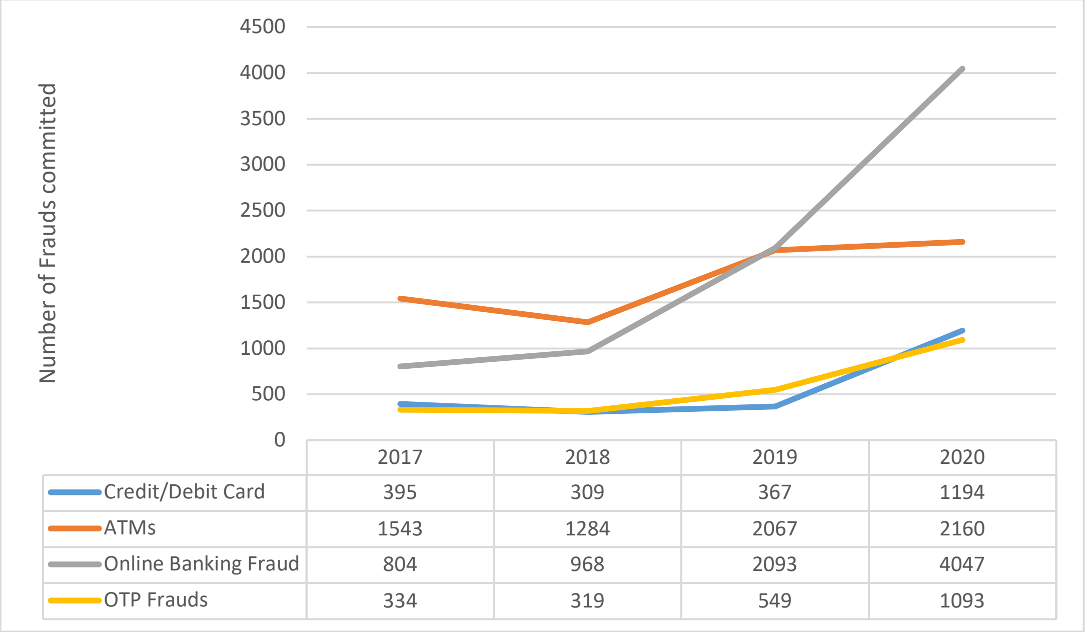
Other crimes which have become advanced because of the internet and technology are Money Laundering, Online Gambling, Cyber Defamation, Cyber Pornography, Intellectual Property Crimes. The criminal act of fraudulently depositing cash in a bank account so as to make it look originating from legitimate source is known as Money Laundering (Hurley, 2020). Online Gambling (aka Internet Gambling) includes any kind of gambling activity which is conducted using the Internet. Famous examples of internet gambling are Virtual Poker, Casinos, Sports Betting, etc. Introduction of Internet has caused commission of cyber defamation an easy task. It is the publication of any defamatory material over the internet be it on social media, blog, or other websites. Defamation done with the help of Internet is called Cyber Defamation. The ever-expanding cyberspace has nurtured the publication of pornographic or obscene content. Cyber Pornography is any activity which includes creation, publication, display, distribution, import of any obscene material. In this information age where the end user can get the information with a single click of the button, the stealing of such information has also become easy. The increasing number of Intellectual Property Crimes is the perfect example of this. Intellectual Property is an umbrella term which is used to refer to Trademarks, Patents, Industrial Design, Literary work, or Artistic work. Whenever someone tries to copy, manufacture, sell or distribute duplicate copy or counterfeit goods including the above-mentioned ones, is termed IP theft. The purpose is to achieve financial gain without the permission or authorization of the original owner/author.

4. Impact on Economy

Technological advancements in the fourth industrial revolution have had a significant impact on increasing the economy of a nation. It has created a globalized world that has virtually erased territorial boundaries between nations. Subsequently, a “new world order” in cyberspace has emerged. This new world order has come up with an increasing number of virtual transactions both intra-national as well as international. The digitization of transactions with the creation of payment gateways on websites and mobile applications have increased the ambit and scope of trade and commerce. Governments actively promote the use of digital payment gateways to keep track of black money.

Another major aspect of digital economy has developed in the form of a virtual asset, also known as cryptocurrency, which functions without the role of any intermediary organization between two persons. The implementation of transactions via cryptocurrencies are regardless of nationalities of the parties. It is based on blockchain technology which is a secure and transparent form of storing critical information. These sophisticated technologies of payments across nations through information and communication technology have given a digital aspect to every country’s economy, known as “Digital Economy”.

No doubt technology has evolved individual economies of the countries into a global digital economy, it has also provided aid to perpetrators who seek to gain monetary benefits through illegal means in the cyberspace. Cybercrimes like banking fraud, OTP frauds, money laundering, skimming, phishing, ATM fraud, ransomware attacks, wire transfer fraud, intellectual property theft, and cyber defamation gravely damage the financial security of an organization and even the economy of a nation. According to NCRB statistics, there has been a constant increase among all kinds of financial crimes (National Crime Records Bureau, 2020). Online Banking Fraud have seen a massive rise of 93.3% within a year from 2019 to 2020 (see Fig. x.2). The data for 2021 has not been published yet, but we can predict based on the curve of this graph and increased number of internet users due to lockdown, that there will definitely be a greater number of crimes than any previous years. This is a matter of concern for Indian Economy.



	2017	2018	2019	2020
Credit/Debit Card	395	309	367	1194
ATMs	1543	1284	2067	2160
Online Banking Fraud	804	968	2093	4047
OTP Frauds	334	319	549	1093

Fig. 2 Banking services as a means of committing cyber frauds. Source Drawn by authors from NCRB (2020)

The European Union (EU) as a collaborative action amongst its member countries, has introduced the Digital Operational Resilience Act (DORA) for a cyber resilient financial infrastructure vis-à-vis risk management and incident reporting (Higbee et al., 2022). Countries like USA, UK and Russia are investing immensely in cyber defense technology for securing their critical infrastructure. India must allocate adequate resources for cyber defense and advancement of technology to secure its economy from cyber-attacks (Data Security Council of India, 2020).

5. Findings and Discussion

India, having the potential to be the third largest economy in the world will also have a target market for cyber-attackers to extract maximum monetary benefits from it. So, while the focus is on developing the economy of the country at the same time there should also be a concern of preserving the future economy from possible cyber-attacks by investing more in cyber security measures. How much more investment needs to be made for securing cyber space might be concluded after analyzing two important aspects, firstly the rate at which India has been incurring financial loss in the past 5 years due to cyber-attacks, and secondly the rate at which cyber-crimes have increased in India over the last 5 years. This might provide us with an estimate of the expenditure that needs to be made for procuring cyber security technology and implementing it at the government level.

Data Security Council of India (DSCI) has provided a comprehensive outlook on areas like digitization of public services, protection of critical information infrastructure, securing digital payments, supply chain security, state-level cyber security, and protecting SMEs. It has also given recommendations on allocating a minimum of 0.25% of the annual budget for cyber security which can be increased up to 1%. Other recommendations include creating cyber security funds for State Governments, allocating around 15-20% of the expenditure in IT for cyber security, organizing workshops & hackathons for promoting research and innovation, and holding drills for a cyber-secure environment (Data Security Council of India, 2020).

6. Conclusion and Recommendation

The ever-changing nature of technology helps hackers to employ dramatically revolutionizing methods to commit sophisticated crimes and damage the critical infrastructure of an economy. They are always one foot forward than the known cyber security tools. Thus, the use of cutting-edge technologies like Artificial Intelligence or a Blockchain technology-based tool will have the potential to minimize the adverse effect on the economy.

It is important for the infosec professional to have knowledge of the present-day threats. They should study the pattern involved in current crimes and predict the future types of cybercrimes. It is a critical step and must be followed so to prevent our data from upcoming digital threats. In the age of Artificial Intelligence along with

Machine Learning algorithms and the increasing number of IoT devices around us, every internet user must be well prepared for the next wave of cybercrime. Cyber security experts in any organization should be given leadership roles in managerial decisions. This would ensure that every organizational decision is made keeping the cyber security aspect of the infrastructure in mind.

However, instead of focusing solely on cyber security, organizations and nations should focus on making their infrastructure more cyber resilient and sustainable. A collective action by the policy makers, international organizations and businesses of the world is needed in todays' time to address the cyber threats proactively and in a sustainable manner. A unanimous, transparent, and democratic global legal framework to combat cyber terrorism needs to be developed with the collaboration and coordination of the United Nations.

India must focus on developing a secure online interactive platform for the healthcare, education, and finance sectors. Making use of blockchain technology to increase information security is a widely accepted solution but what challenges will it face during its implementation, both technical as well as legal has scope for future research. A harmonious working of the government with various search engines, intermediaries, VPN providers, and the likes would better resolve the information security hurdles which take place in cyberspace. The National Cyber Security Strategy which was introduced in the year 2020 by DSCI needs a fast-track implementation now more than ever. Allocation of resources and investments in cyber-defense must increase. Along with a defensive approach, India must also strengthen itself in terms of projecting a proactive cyber response to protect its critical infrastructure from damage. A special law must be formulated by the Parliament to address the cyber security concerns of the citizens and the integrity of the nation. This law must impose an obligation of complying with cyber safety measures upon the players dealing with sensitive data. The law must also provide for the establishment of exclusive courts to resolve matters of cybercrimes and cyber security. In this way the effect of cybercrimes on different stakeholders can be minimized, which will ultimately be beneficial for the economic growth of the country.

References

Abrigo. (2013). *A study of new wire fraud schemes, how they impact community financial institutions and how you can help stop it.* https://www.abrigo.com/wp-content/uploads/2019/01/WPaper-Wire-Fraud.pdf

Acharjee, S. (2021, February 13). *The evolution of cybercrime: An easy guide(2021)*. Jigsawacademy. https://www.jigsawacademy.com/blogs/cyber-security/evolution-of-cybercrime/

Bissell, K., & Pipikaite, A. (2022). *Everything you need to know about cybersecurity in 2022*. World Economic Forum. https://www.weforum.org/agenda/2022/01/cyber-security-2022-global-outlook/

Blackstone, W. (1769). *Commentaries on the laws of England* (Vol. 4). University of Chicago Press. https://press.uchicago.edu/ucp/books/book/chicago/C/bo3620085.html

Chantzos, I. (2022). *New regulatory requirements will help shape cyber security for finance*. Broadcom Software. https://symantec-enterprise-blogs.security.com/blogs/feature-stories/how-new-regulatory-requirements-will-shape-cyber-security-finance-sector

Data Security Council of India. (2020). *National cyber security strategy 2020*. https://www.dsci.in/sites/default/files/documents/resource_centre/National Cyber Security Strategy 2020 DSCI submission.pdf

De', R., Pandey, N., & Pal, A. (2020). Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management*, *55*(June), 102171. https://doi.org/10.1016/j.ijinfomgt.2020.102171

De Groot, J. (2019). *What is cyber resilience?* Digital Guardian. https://digitalguardian.com/blog/what-cyber-resilience

Dennis, M. A. (2019). *Cybercrime*. Encyclopedia Britannica. https://www.britannica.com/topic/cybercrime

Department of Land Resources. (2022). *Detailed demands for grants 2022-2023*. https://dolr.gov.in/en/document/detailed-demands-grants-year-2022-2023-corrigendum-dated-15th-march-2022

Dewi, P. E. T., & Septiwidiantari, N. M. (2021). Efforts to overcome criminal acts of skimming committed through ATMs in the perspective of law number 19 of 2016 concerning EIT. *Jurnal Notariil*, *6*(2), 106–111. https://doi.org/10.22225/jn.6.2.2021.106-111

Dieselcafe. (2014, January 8). *Life at 6700': Research paper - The rise of cybercrime 1970s - 2010*. DieselCafe. http://www.dieselcafe.com/2014/01/research-paper-rise-of-cybercrime-1970s.html

Forum, W. E. (2017). *The global risks report 2017: 12th Edition*. World Economic Forum. https://www3.weforum.org/docs/GRR17_Report_web.pdf

Higbee, A., Erenhouse, R., Doyle, S., & Nezurugo, M. P. (2022, March 28). *Assessing the need for global cybersecurity regulations*. World Economic Forum. https://www.weforum.org/agenda/2022/03/why-global-harmonisation-of-cybersecurity-regulations-would-be-like-music-to-our-ears/

Hurley, C. (2020). *Identifying and responding to wireless attacks*. Blackhat. https://www.blackhat.com/presentations/bh-jp-05/bh-jp-05-hurley/bh-jp-05-hurley.pdf

Indian Computer Emergency Response Team. (2022). *CERT-In annual report (2021)*. *April*. https://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT

Karamchand Gandhi, V. (2012). An overview study on cyber crimes in internet. *Journal of Information Engineering and Applications*, *2*(1). https://core.ac.uk/download/pdf/234676934.pdf

Kratikal. (2019, November 1). *5 biggest cyber attacks in India*. Kratikal Blogs. https://www.kratikal.com/blog/5-biggest-cyber-attacks-in-india/

Kshetri, N. (2013). Cybercrime and cyber-security issues associated with China: Some economic and institutional considerations. *Electronic Commerce Research*, *13*(1), 41–69. https://doi.org/10.1007/s10660-013-9105-4

Kulkarni, S. (2022, March 25). 10 types of banking frauds in India customers should know about. *The Economic Times*. https://economictimes.indiatimes.com/wealth/save/10-types-of-banking-frauds-in-india-customers-should-know-about/articleshow/90438911.cms

Mint. (2021, December 26). *India to become 3rd largest economy in 2031, says CEBR*. Livemint. https://www.livemint.com/economy/india-to-become-3rd-largest-economy-in-2031-says-cebr-11640510927249.html

Nappo, S. (2019). *Cybercrime quotes*. GoodReads. https://www.goodreads.com/author/quotes/19698507.Stephane_Nappo

National Crime Records Bureau. (2015). *Cases reported and persons arrested under cyber crime and their percentage variation in 2015 over 2014 (State/UT-Wise)*. https://ncrb.gov.in/sites/default/files/Statistics/Statistics-2015_rev1_1.pdf

National Crime Records Bureau. (2016). Cyber crimes incidence & crime rate (state/UT-wise). In *Ministry of Home Affairs*. http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/NEWPDFs/Crime in India - 2016 Complete PDF 291117.pdf

National Crime Records Bureau. (2017). Cyber crimes (state/UT-wise). In *Ministry of Home Affairs*. https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/Table 9A.1_2.pdf

National Crime Records Bureau. (2018). *Cyber crimes (state/UT-wise)* (Vol. 2). https://ncrb.gov.in/sites/default/files/Crime in India 2018 - Volume 2.pdf

National Crime Records Bureau. (2019). Cyber crimes (state/UT-wise). In *National Crime Records Bureau*. https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/Table 18.1_2015.pdf

National Crime Records Bureau. (2020). Cyber crimes (state/UT-wise). In *Ministry of Home Affairs*. https://ncrb.gov.in/sites/default/files/crime_in_india_table_additional_table_chapter_reports/TABLE 9A.1.pdf

News18. (2019, August 10). India ranked highest in IoT cybersecurity attacks last quarter: Report. *News18*. https://www.news18.com/news/tech/india-ranked-highest-in-iot-cybersecurity-attacks-last-quarter-report-2265951.html

O'Murchu, L. (2022). *How cyber security is changing in the post-pandemic era*. Symantec. https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/how-cyber-security-changing-post-pandemic-era

Prakash, A., & Singh, A. (2021). *Cyber security: Issues and challenges in Covid - 19*. https://doi.org/10.3390/mol2net-07-10318

Press Information Bureau. (2018, December 18). *Cyber security*. Ministry of Home Affairs. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1556474

Rajput, B. (2020). Cyber economic crime in India. In *Springer Series on Asian Criminology and Criminal Justice Research*. http://link.springer.com/10.1007/978-3-030-44655-0

Reserve Bank of India. (2022). *BE(A)WARE – A booklet on modus operandi of financial frauds*. Reserve Bank of India. https://rbidocs.rbi.org.in/rdocs/content/pdfs/BEAWARE07032022.pdf

Sadie, C., Jamie, S., Louse, A., & William, D. (2020). Cybersecurity, emerging technology and systemic risk.

Future Series, *November*, 59. https://www.weforum.org/reports/future-series-cybersecurity-emerging-technology-and-systemic-risk

Sharma, A., & Krishna Pallavi, V. (2017). Restorative justice: A complement to the prevailing criminal justice system. *D Roit P Enale: Indian Law Journal on Crime & Criminology (Online)*, *1*(2). https://www.scribd.com/document/452647144/9-pdf

Sharma, Y. S. (2022, February 25). *India can be 3rd largest economy by 2030 on back of four big reforms: Arvind Panagariya - The Economic Times*. ET Bureau. https://economictimes.indiatimes.com/news/economy/indicators/india-can-be-3rd-largest-economy-by-2030-on-back-of-four-big-reforms-arvind-panagariya/articleshow/89834954.cms

Sviatun, O. V., Goncharuk, O. V., Chernysh, R., Kuzmenko, O., & Kozych, I. V. (2021). Combating cybercrime: Economic and legal aspects. *WSEAS Transactions on Business and Economics*, *18*, 751–762. https://doi.org/10.37394/23207.2021.18.72

Teoh, C. S., & Mahmood, A. K. (2018). Cybersecurity workforce development for digital economy. *The Educational Review, USA*, *2*(1), 136–146. https://doi.org/10.26855/er.2018.01.001

Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, applications and opportunities. *International Journal of Information Management*, *54*(March 2019), 102120. https://doi.org/10.1016/j.ijinfomgt.2020.102120

World Economic Forum. (2020). *Centre for cybersecurity*. World Economic Forum. https://www.weforum.org/platforms/the-centre-for-cybersecurity