Research Journal of Forensic Sciences ISSN 2321–1792
Vol. **12(1),** 9-15, January **(2024)** *Res. J. Forensic Sci.*

Socio-Economic Conditions of Cybercrime Victims in India: A Study of Karnataka State, India

Purnanand N. Sangalad
Department of Criminology and Forensic Science, Karnatak University's, Karnatak Science College, Dharwad- 580 001, Karnataka, India
sangaladkcd@gmail.com

Available online at: www.isca.in, www.isca.me
Received 21th August 2023, revised 26th October 2023, accepted 4th December 2023

Abstract

Contemporary Socio-Economic environment is evolving becoming more security conscious. Currently people are taking a greater number of steps to get safety and security from both the government and the industry including online services. A dual economy, low income and educational levels, which result in poor levels of human development, high unemployment rates, high levels of income inequality, and flimsy democratic institutions are some of the main economic and social traits of a developing nation. Just as there are many different kinds of crimes that can be done, so too can the types of people that perpetrate cybercrimes. Cybercriminals can include young hackers, resentful workers and insiders, or foreign terrorists and spies. When a computer is used in their crimes, these criminals become into cybercriminals. It goes without saying that cybercrime is a major problem in Karnataka, costing the state and its people a great deal of money. The fact that criminals are frequently effective in hiding their identities is the most pressing issue. The commonest Cybercrime observed was the Cyber stalking and least encountered was the Morphing. Victim being the commonest manner of Cyber stalking (54%) with residing in Urban setup belonging to Middle socioeconomic strata (53.34%).

Keywords: Socio-Economic, Cybercrime, Victim, Criminal, Computer, Internet.

Introduction

The contemporary socio-economic environment is evolving and becoming more security conscious. Currently people are taking a greater number of steps to get safety and security from both the government and the industry including online services. These changes create a new era of security known as information technology security. A dual economy, low income and educational levels, which result in poor levels of human development, high unemployment rates, high levels of income inequality, and flimsy democratic institutions, are some of the main economic and social traits of a developing nation[1,2]. We contend that there is a close relationship between these traits and cybercrime. Many times, these reasons transcend between social- economic, behavioural and psychological personal factors[3].

For example, low income and education levels cause consumers and developing world-based enterprises to adopt new technologies very slowly. Since many of the people in the developing world only recently acquired computers and made their first Internet connection, many of them lack technical knowledge and experience. Most of them are also not fluent in English. Because the majority of security product instructions, information, and other elements are only available in English, this last point is quite important. A large number of Internet users in developing nations are unable to use IT security products that are written in English[4].

A dual economy can be defined as having two sectors: an industrialized urban sector that is reasonably developed and a rural sector[2]. Because of the dual character of the economy, developing economies are also distinguished by uneven development within a particular sector, in addition to variation between economic sectors. Targeting emerging markets, cybercrimes typically concentrate in well-established industry areas, such as the Chinese online gaming market, the Brazilian banking and financial sector, and the Indian outsourcing market[4].

Just as there are many different kinds of crimes that can be done, so too can the types of people that perpetrate cybercrimes. Cybercriminals can include young hackers, resentful workers and insiders, or foreign terrorists and spies. When these criminals employ computers in their crimes, they turn into cybercriminals. A computer could be the target of a criminal, or alternatively, the computer could be the object of the crime. A computer may also be the target of a crime, or to put it another way, the actual location of the crime or the cause of some types of asset loss. Examples of this kind of criminal activity include sniffers, logic bombs, and viruses. And last, the tool "used to commit traditional crimes" may be a computer. Identity theft is the most prevalent cybercrime that may be perpetrated via a computer, for instance. Nowadays, identity theft is referred to as the digital era's trademark crime[5].

With technology seeping in the modern times, the knowledge about operating the mobile and internet is very basic and

primitive that, now a child of an average age of 10 can use the mobile to comprehend question, read about current affairs and play. The information flow has risen due to the increased exposure of young adults in this age group to electronics and technology, but it has also created more opportunities for online deviant behaviours like cybersex ting, online stalking and sexual harassment, and fraud. Despite encouraging support for free internet, technology and the internet have given rise to a platform where abnormal behaviour can flourish, which has created an environment that is ideal for these kinds of cybercrimes. Younger generation given the age they are in and sudden outburst of hormones directly related to puberty and with their inquisitive mind towards the new technology and its use makes youths more susceptible to such kind of crimes[6,7].

As technology and the economics have advanced, the internet has become increasingly important in our daily lives. Cybercrime is a phenomenon that affects society and the economy. The information technology sector is one of the major growth drivers for the Indian economy and an engine of prosperity and expansion. This industry not only supports India's economy but also improves people's lives by directly and indirectly affecting a number of socioeconomic indicators, including employment, standard of living, and diversity. Given that the likelihood of encountering a cyber attack is closely correlated with the extent to which economic activities are digitalized[8], India should be commended for its enormous digitization initiatives. The industry has made a significant contribution to changing the perception of our nation as a major player on the international stage offering top-notch business services and technological solutions[9]. Over 50 countries have formally released plans to combat potential cyber attacks, cybercrime, and/or cyber security threats[10]. The term "cyberspace" was initially used by William Gibson in his literary work "Neuromancer", which discussed electronic activities that occur in virtual worlds. The "Space Transition Theory" was developed by Jaishankar to explain the reasons behind cybercrimes. The thesis, which consists of seven postulates, describes how a person's behaviour varies in real and virtual spaces and how this could result in crimes being committed in virtual spaces[11]. The US Department of Justice, for example, classifies cybercrimes as "forms of crimes that involve computers and networks" in general[12]. Parthasarthi defined cybercrime as “an illegal activity that uses computer to commit crime”[13].

A different estimate estimated that 42 million Indians were victimised online in 2011. The Norton Cybercrime Report of 2011 stated that 30 million Indians have become victims of cybercrime, costing the Indian economy $7.6 billion annually[14]. Additionally, India has been the victim of well-known international cyber attacks. For example, the Stuxnet virus affected computers in India even though its intended purpose was to harm Iran's centrifuges at the nuclear site in Natanz[15]. India is also the source of a substantial number of cybercrimes that affect Internet users worldwide. For instance, the top country of origin for spam in 2011 and 2012 was India[16,17]. Similarly, in the second half (H2) of 2011, India had the highest phishing TLDs by domain score (determined as phish per 10,000 domains), according to a phishing survey published by the Anti-Phishing Working Group (APWG) in April 2012[18]. India is one of the top non-North American countries from where click fraud originates[19]. India was sixth in terms of the quantity of complaints that the U.S. based Internet Crime Control Centre received[20].

Since each cybercrime is unique, it is impossible to define the term "cybercrime" precisely. Actually, the word "cybercrime" is a general one that describes any illegal activity carried out through a computer and the internet. But mostly, it refers to crimes that are done online, that is, when the victim and the perpetrator are both connected via the World Wide Web (WWW). Thus, crimes that target a computer or computer resource or those are done using a computer as a tool are considered cybercrimes.

Strict definition of cybercrime cannot be found in the IT act, 2000 or even the IT (Amendment) Act, 2008. In fact, the definition does not occur in any legislation in India. Going by the dictionary definition, a cybercrime may be said to be any criminal act that involves a computer, or a mobile, or similar electronic instruments of communication as a tool for the commission of the offence or as a target of the committed offence or both[21].

As on June 2012, India stood third in the world with respect to the percentage of Internet users. Internet users in India account for 17.2% of the global percentage, while China tops the list by contributing a massive 22% and the U.S., surprisingly, comes third with a contribution of 4.42%. India is experiencing an increase in cybercrime, similar to many other nations. In 2018, 208, 456 cyber-related offences were reported. More cybercrimes were reported in the first two months of 2022 than in the whole of 2018. Throughout the epidemic, the numbers increased even more dramatically, with reported crime rising from 394,499 cases in 2019 to 1,158,208 cases in 2020 and 1,402,809 crimes in 2021. India had a 15.3% rise in cybercrime between Q1 and Q2 of 2022. In addition, the number of Indian websites that have been hacked in recent years has been rising. In 2018, there were approximately 17,560 hacks. 26,121 more websites were compromised in 2020. In 2021, ransom ware attacks affected 78% of Indian organizations, with data encryption occurring in 80% of those cases. By contrast, the average attack percentage was 66% and the average encryption rate was 65% [22].

Notably, during the course of the last 10 years, at least three pertinent review studies have called attention to the deficiencies and current condition of cybercrime research[23-25]. Examining both formal and informal institutions is vital to shed light on India's poor prosecution and conviction rates for cyber-offenders. Researchers from the past have acknowledged that

both formal and informal institutions contain economic players and activity[26,27]. Another issue to consider is that the types of operations that cybercriminals engage in are quite similar to what Baumol refers to as destructive entrepreneurship[28]. According to Baumol's theory, the rewards that society's norms of conduct bestow on entrepreneurs-productive, unproductive, and destructive-determine how these entrepreneurs are distributed. We refer to these regulations as institutions[29].

High unemployment rates, significant income disparity, inadequate democratic institutions, low income and educational levels, which result in low levels of human development, and a dual economy are some of the main economic and social traits of emerging nations[30]. We contend that there is a close relationship between cyber security and cybercrime.

Low income and education levels, for example, cause customers and developing world-based firms to adopt new technology relatively slowly. Since a large percentage of people in developing nations recently acquired computers and made their first Internet connections, many of them lack technological know-how and experience. The vast majority of them are also not proficient in the English language. This latter aspect is particularly important because the majority of security product instructions, information, and other elements are only available in English. A large number of Internet users in developing nations are unable to use IT security products that were created in English[19-21].

A dual economy can be defined as having two sectors: an industrialized urban sector that is reasonably developed and a rural sector[31]. Because of the dual character of the economy, developing economies are also distinguished by uneven development within a particular sector, in addition to variation between economic sectors[32]. Targeting emerging markets, cybercrimes typically concentrate in well-established industry areas, such as the Chinese online gaming market, the Brazilian banking and financial sector, and the Indian outsourcing market[33].

After doing a literature review, Acemoglu & Acemoglu et al[34,35] have determined the basic and immediate origins of both wealth and poverty. Table-1 lists these, and the final column demonstrates how some of them are connected to cyber security and cybercrime in India.

Cybercrime has been trending upwards in Karnataka[36,37]. Technically qualified cyber criminals are interested in new patterns of crime using new technologies. It goes without saying that cybercrime is a major problem in Karnataka, costing the state and its people a great deal of money. The fact that criminals are frequently effective in hiding their identities is the most pressing issue[38]. Figure-1 displays the total number of cybercrimes in Karnataka State that were reported to the National Crime Records Bureau between 2012 and 2021[39]. But as many crimes go unreported, this does not fairly represent the total number of crimes committed.

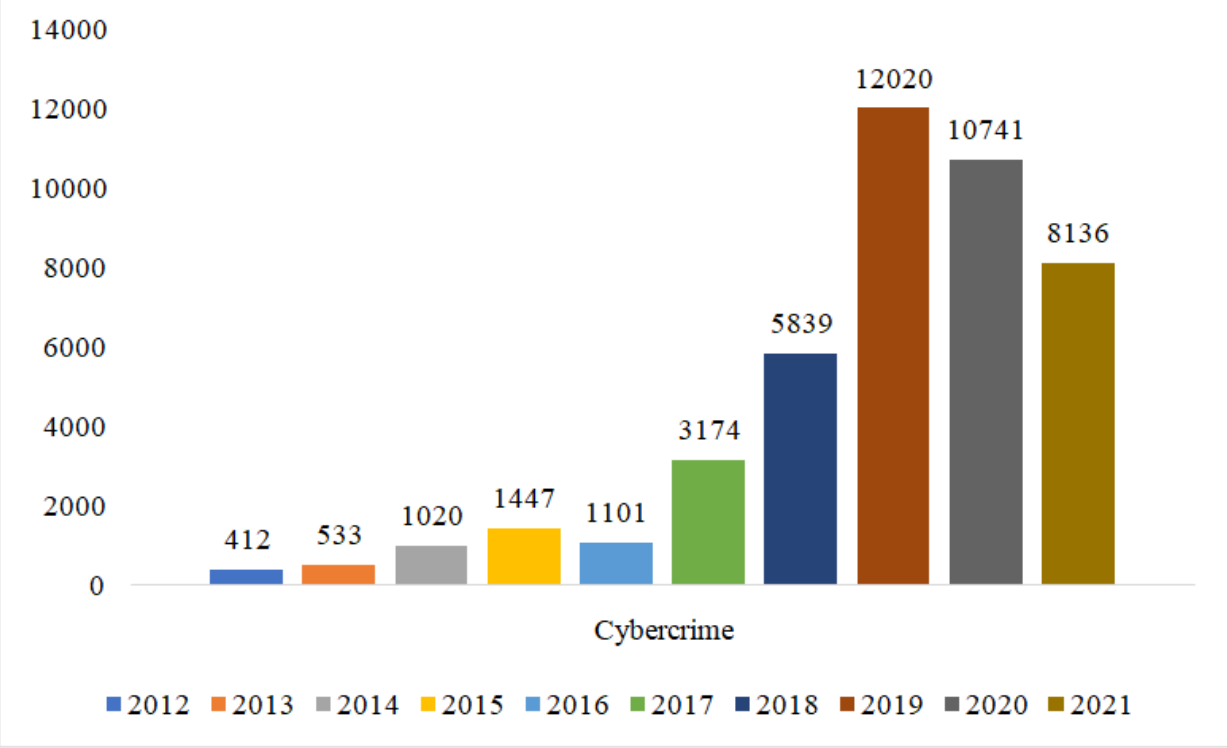

Figure-1: Total number of cybercrimes reported in Karnataka State (2012–2021)[39].

Objectives of the Study: The goal of the current study was to investigate the socio-economic circumstances and situation of the families of cybercrime victims.

Materials and Methods

Primary data are the major source of information used in this study. 1500 Cybercrime victims' families (2011-2012 to 2021-2022) were collected from Conditions of Cybercrime victim families in Karnataka State. The respondents were surveyed using structured questionnaires to collect data. Statistical tools were utilised to evaluate and interpret data pertaining to cybercrime victims' families that were gathered from 30 districts throughout the state of Karnataka.

The purpose of this review is to summarise the most recent research on the social and economic effects of cybercrime in the state of Karnataka as well as the obstacles to the efficient implementation and execution of the state's cybercrime laws.

Results and Discussion

Among 1500 cases of Cybercrime victim studied during 2011 - 2022, majority of the victims were in the age group of 41-50 (37.33%), the commonest type of Cybercrime (54%) encountered was Cyber stalking (Table-1). The commonest manner of Cybercrime was victim were in the gender of females (53.33%) followed by Cyber stalking victim accounting for 54% in male and female respectively. Most of the victims belonged to Urban area i.e. 1100 (73.33%) in comparison to rural area (26.67%). Persons of middle socio-economic strata are the commonest victims (53.34%) followed by upper class (30%) and lower class (16.66%) least involved (Table-3). Figure-1 above depicts the years 2019 and 2020, when Karnataka state reported higher rates of cybercrime due to the COVID-19 epidemic. Due to everything that involves online shopping.

Nowadays, there are three ways to interpret the term "modernization": (1) as the internal growth of the European New Era in Western Europe and North America; (2) as the process by which non-first group countries try to catch up with them; and (3) as the evolutionary development of the most modernised societies (Western Europe and North America); that is, modernization as a continuous process carried out through innovation and reform that today denotes a shift to a post-industrial society[40].

The commonest Cybercrime observed was the Cyber stalking and least encountered was the Morphing. This is consistent with the observations made by earlier studies. Victim being the commonest manner of Cyber stalking (54%) with residing in Urban setup belonging to Middle socioeconomic strata (53.34%). This is possibly due to illiteracy and poverty of the modernization in urban parts. They solely depend on the job for government, non-governmental and business income for their livelihood. Due to some reason (i.e. either lack of knowledge of computer or mobile phone) if they are not able to generate the required knowledge of using of online purchasing things for their day to day living and commitments, they may get Cybercrime and resort to victimised.

Table-1: Shows age wise, common type of cyber-crime faced among the victims of Karnataka state.

Age	No, of Cybercrime victim	Types of Cybercrimes faced	No, of Cybercrime victim
0-10	0 (0)	Cyber stalking	810 (54)
11-20	30 (2)	Harassment via email	300 (20)
21-30	25 (1.67)	Cyber defamation	40 (2.66)
31-40	60 (4)	Morphing	30 (2)
41-50	560 (37.33)	Email spoofing	120 (8)
51-60	475 (31.66)	Hacking	50 (3.34)
61-70	200 (13.34)	Cyber flirting	150 (10)
71 above	150 (10)	Total	1500 (100)
Total	1500 (100)		

Table-2: Shows gender wise, common type of Cybercrime distribution among the victims of Karnataka State.

Gender	No, of Cybercrime victim
Male	800 (53.33)
Female	700 (46.67)
Total	1500 (100)

Table-3: Shows manner of Cybercrime, affected areas and socio-economic status of Cybercrime distribution among the victims of Karnataka State.

Areas	No, of Cybercrime victim	Economic Status	No, of cybercrime victim
Rural	400 (26.67)	Lower class	250 (16.66)
Urban	1100 (73.33)	Middle class	800 (53.34)
Total	1500 (100)	Upper class	450 (30)
		Total	1500 (100)

Throughout the past year, there has been a noticeable increase in cybercrime in the form of well-publicized ransom ware campaigns. Massive breaches exposed people to fraud by leaking personal data, while the Wanna Cry ransom ware attack disrupted services and endangered lives, affecting the NHS and numerous other businesses throughout the globe. Strategies are changing right now because businesses are being targeted more often than individuals, and although while the number of people falling victim to phishing attempts is rising, people are becoming more vigilant.

In most cases, lone people or small groups perpetrate cybercrimes. Big organized crime gangs do, however, also utilize the Internet. These "professional" criminals create international criminal networks and devise inventive ways to carry out time-honoured crimes, such as cybercrime.

Criminal groups might band together to undertake coordinated attacks by exchanging tactics and equipment. Cybercriminals can purchase and trade identities and stolen data on their underground marketplace. Because the Internet makes it simpler for people to conduct things anonymously and from anywhere in the world, it is exceedingly difficult to take action against cyber criminals. In reality, many of the machines used in cyber attacks have been compromised and are under the control of a remote attacker. Every country has a different set of crime laws, which can make things extremely difficult when a criminal attack another nation.

Conclusion

The same article contained accurate predictions about the rise in cell phone time theft and phone fraud, the use of biometrics and encryption to protect data in cyberspace, the rise in cyber attacks and fraud against government and business, the massive theft and fraud of credit cards, the internal theft of clients' identities by financially struggling and/or avaricious financial service employees.

Cybercrimes are also on the rise in tandem with the rise in internet users. Everyday life is full of many types of cybercrimes. However, not everyone is aware of all of these kinds. The majority of people just have knowledge of viruses and worms and hacking. They don't know about identity theft, phishing, defamation, cyber stalking, etc. Understanding these crimes connected to the internet is essential in today's environment.

References

1. UNDP (2006). Country evaluation: Assessment of development results Honduras, New York: United Nations Development Programme Evaluation Office. Retrieved from http://web.undp.org/evaluation/documents/ADR/ADR_Reports/ADR_Honduras.pdf.

2. Lewis, A. (1954). Economic development with unlimited supplies of labour. *Manchester School of Economic and Social Studies*, XXII (May 1954), 139–91.

3. P.N. Sangalad, (2012). Farmers' Suicides in India as an Socio-Economical Phenomenon: A Study of Karnataka State. *International Journal of Criminology and Sociological Theory*, 5(3), 964- 971.

4. Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies. *Third World Quarterly*, 31(7), 1057-1079.

5. Chenery, H. B. (1975). The structuralist approach to development policy. *The American Economic Review*, 65(2), Papers and Proceedings of the Eighty-seventh Annual Meeting of the American Economic Association, 310–316.

6. Choi, K. (2015). Cyber-criminology and digital investigation. El Paso: LFB Scholarly Publishing LLC.

7. Wolak, J., Mitchell, K. J., & Finkelhor, D. (2006). Online Victimization of Youth: Five Years Later.

8. Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. *Communications of the ACM*, 52(12), 141-144.

9. GOI (2015). Ministry of Electronics & Information Technology, Government of India. http://meity.gov.in/sites/upload_files/dit/files/ncsp_060411.pdf last visited 13/08/2015

10. Klimburg, A. (Ed.). (2012). National cyber security framework manual. NATO Cooperative Cyber Defense Center of Excellence.

11. Jaishankar, K. (2008). Space transition theory of cyber crimes, crimes of the internet.

12. Punia, C. K. (2009). Cyber Laws. New Delhi: Sumit Enterprises.

13. Paranjape, N. (2012). Criminology and Penology with Victimology, Allahbad.

14. Anonymous, (2012). India battles against cybercrime. Retrieved from http://www.indolink. com/displayArticleS.php?id=102112083833.

15. Rid, T. (2012). Think again: cyber war. Foreign Policy, (192), 80.

16. Anonymous (2012). Spam capital' India arrests six in phishing probe. Retrieved from http://www.bbc.co. uk/news/technology-16392960.

17. King, R. (2011). Cloud, mobile hacking more popular: Cisco. Retrieved from http://www.zdnet. com/cloud-mobile-hacking-more-popular-cisco-1339328060/.

18. Aaron, G., Rasmussen, R., & Routt, A. (2012). Global phishing survey: Trends and domain name use in 2H2011, APWG. http://www.antiphishing.org/reports/APWG_ Global PhishingSurvey_2H2011. pdf.

19. Kshetri, N. (2010). The economics of click fraud. *IEEE Security & Privacy*, 8(3), 45-53.

20. Internet Crime Complaint Center (2011). 2010 internet crime report. Retrieved from http://www.ic3. gov/media/annualreport/2010_ic3report.pdf.

21. AAG IT Services (2023). The latest cyber crime statistics. https://aag-it.com/the-latest-cyber-crime-statistics/ 2023

22. Internet World Stats (2016). Top 20 Countries with the Highest Number of Internet Users. available at accessed on 7 July, 2016.

23. Bossler AM. (2017). Need for debate on the implications of honeypot data for restrictive deterrence policies in cyberspace. *Criminol*. Public Policy, 16, 681–88.

24. D'Arcy J. and Herath T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *Eur. J. Inf. Syst*., 20, 643–58.

25. Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant behavior*, 35(1), 20-40.

26. Granovetter, M., Action, E., & Structure, S. (1985). The problem of embeddedness. *American journal of sociology*, 91(3), 481-510.

27. Parto, S. (2005). Economic activity and institutions: Taking Stock. *Journal of Economic Issues*, 39(1), 21–52.

28. Baumol, W. J. (1990). Entrepreneurship: Productive, unproductive, and destructive. *Journal of Political Economy*, 98(5), 893–921.

29. North, D. C. (1990). Institutions, institutional change and economic performance. Cambridge: Harvard University Press.

30. UNDP (2006). Country evaluation: Assessment of development results Honduras, New York: United Nations Development Programme Evaluation Office. Retrieved fromhttp://web.undp.org/evaluation/documents/ADR/ADR_Reports/ADR_Honduras.pdf.

31. Lewis, A. (1954). Economic development with unlimited supplies of labour. Manchester School of Economic and Social Studies, XXII (May 1954), 139–91.

32. Chenery, H. B. (1975). The structuralist approach to development policy. The American Economic Review, 65(2), Papers and Proceedings of the Eighty-seventh Annual Meeting of the American Economic Association, 310–316.

33. Kshetri, N. (2010). Diffusion and effects of cybercrime in developing economies. Third World Quarterly, 31(7), 1057–1079.

34. Acemoglu, D. (2005). Political economy of development and underdevelopment. Gaston Eyskens Lectures, Leuven, Department of Economics, Massachusetts Institute of Technology, Retrieved from http://economics.mit.edu/files/1064.

35. Acemoglu, D., Johnson, S., & Robinson, J. A. (2005). Institutions as a fundamental cause of long-run growth. *Handbook of economic growth*, 1, 385-472.

36. Datta, P., Panda, S. N., Tanwar, S. and Kaushal, R. K. (2020). A technical review report on cyber crimes in India. In 2020 International Conference on Emerging Smart

Computing and Informatics (ESCI), 12–14 March 2020, Pune, India, eds., 269–275. Piscataway, NJ: Institute of Electrical and Electronics Engineers (IEEE). https://doi.org/10.1109/ ESCI48226.2020.9167567

37. Kethineni, S. (2020). Cybercrime in India: Laws, regulations, and enforcement mechanisms. In The Palgrave handbook of international cybercrime and cyber deviance, eds. Holt, T. and Bossler, A., 305–326. London: Palgrave Macmillan. https://doi. org/10.1007/978-3-319-78440-3_7

38. Joshi, Y. and Singh, A. (2013). A study on cybercrime and security scenario in India. *International Journal of Engineering and Management Research*, 3(3), 13–18.

39. NCRB (2021). National Crime Records Bureau. Minister of Home Affairs New Delhi (2021)

40. Gavrov, Sergey; Klyukanov, Igor (2015). Modernization, Sociological Theories of". In Wright, James D. (ed.). International Encyclopedia of the Social &Behavioral Sciences. Vol. 15 (2nd ed.). Oxford: Elsevier Science. pp. 707–713.