Indian Journal of Forensic Medicine and Toxicology
Volume 16 No. 4, October-December 2022

Cyber Crime and Role of Law Enforcement to Tackle Online Crime in Jammu and Kashmir

Tahir ul Gani Mir[1], Aasif Hussain Sheikh[2]

[1]Research Scholar, School of Bio-Sciences and Bio-Engineering, Lovely Professional University, Phagwara Jalandhar, Punjab, 144411, [2]Research Scholar, School of Social Sciences, University of Kashmir, Hazratbal, Srinagar, Jammu, and Kashmir, 190006.

How to cite this article: Tahir ul Gani Mir, Aasif Hussain Sheikh. Cyber Crime and Role of Law Enforcement to Tackle Online Crime in Jammu and Kashmir. Indian Journal of Forensic Medicine and Toxicology 2022;16(4).

Abstract

Since the inception of the computer the cybercrime cases have been reported by and large. However, with easily accessible internet services, lawlessness has gained momentum across the world. The infractions are enacted in diverse forms like banking frauds, hacking, online piracy, stealing of IPRs, match-fixing, etc. This review provides comprehensive insights into the cyber crimes across Jammu and Kashmir with illustrations of the copious number of reported crimes. An inclusive and extensive description of criminality in the modern world makes this review indispensable and significant. The numbers presented in the review are precisely unerring and easy to understand. From fake news reporting to social media craziness this review vastly touches the necessary aspects of the cybercrime doldrums.

Keywords: Cybercrime, E-Crime, India, Jammu and Kashmir, Police

Introduction

Cybercrime is the latest and potentially the most complex epidemic in the history of technology. The concept of cybercrime involves any criminal activity that uses a computer as a subject or object, target or medium to reinforce further crimes. Cybercrime can be described in simple words as any criminal act where computers could be used as a weapon or target. Computers may be used to commit a crime in several ways like illegal access to the device, stealing of electronics-related information, e-mail bombing, data mining, salami attacks, logic bombing, Trojan attacks, web-time theft, computer-based theft, physical damage to the computer system, etc.[1]. At the 10th United Nations Congress on Crime Treatment and Control of Offenders, devoted specifically to computer-related crime, cybercrime was divided into two categories, I- Cybercrime in a limited sense: any illegal activity involving online operations that affects the security of the computer network and the data created by it. II- Cybercrime in a broader sense: Any illegal action carried out on or in conjunction with a computer system or network, including offences like unlawful possession and the collection or distribution of unauthorized information through a computer system or network[2]. Literature studies have established the following four forms of cybercrime

Corresponding Author: Tahir ul Gani Mir, Research Scholar, School of Bio-Sciences and Bio-Engineering, Lovely Professional University, Phagwara Jalandhar, Punjab, 144411.

E-mail: mirtahir4u@gmail.com

1. Use of Computers as a target to commit the crime: stealing of intellectual property, hacking of marketing information like client list, pricing info or promotional plan, and accessing computer files for blackmailing purposes (e.g. Personal data, medical information or sexual preference).
2. Use of Computers as a tool of crime: fraudulent use of credit/debit cards; illegal money transfers, illegal stock sales, etc.
3. Use of Computers associated with other crimes: money laundering and fraudulent bank transactions, organized crime reports or documents, match-fixing in sports, etc.
4. Crime correlated with computer prevalence. -Piracy / counterfeit apps, copyright theft, counterfeit goods, black-market hardware and systems, burglary of electronic gadgets, etc.[3]

Common Forms of Cyber Crime

Throughout all times, cybercrimes cost businesses and people billions and billions of dollars annually. Perhaps more appalling is the fact that this statistic still had no limit in sight for the past five years. The advancement of technology and greater usability of intelligent technology ensures that hackers can use multiple access points to get into the user's online profiles. although law enforcement continues to counter this massive concern, there are still many offenders exploiting Internet anonymity. Below are the most common forms of cybercrime that are continuously growing rapidly.

1. **Hacking**- Hacking is an act performed by an attacker by accessing the computer device without proper consent. Hackers are essentially computer programmers with sophisticated programming expertise and usually misusing this information for illegal acts. They are typically technology experts with expert-level expertise in one program or another. The motives behind hacking may be greed, popularity, money, etc. Most of the hackers do it simply to show their expertise. In most common cases hacker breaks into systems to steal personal banking information, financial records, etc. They often try to modify processes so they can perform tasks at their will. Hackers with such aggressive activity are often called black hat hackers. On the other side are 'White Hat' hackers, who condemn computer system misuse. another term is 'Grey hat' hackers who may sometimes violate laws and have malicious intent as that of black hat hackers[4,5].
2. **SQL (Structured Query Language) Injections:** An SQL injection is a technique that enables hackers to exploit a security vulnerability in the software. This could be used to target any unprotected or insecure SQL database This method includes inserting SQL code into a web form entry field (usually usernames and passwords), to allow the intruder more exposure to the database of the website or a particular account. It may also be used to collect details including credit card numbers or passwords from insecure pages[6].
3. **Cross-site Scripting (XSS)-** Cross-site Scripting is an injection attack on client-side code. The attacker aims to execute malicious scripts in the victim's web browser by inserting malicious code into the website. The actual attack happens as the victim visits the website or application that executes the malicious code. The web page or application serves as a tool for distributing malicious scripts to the user's browser. Vulnerable platforms typically used for such attacks are shopping offer web links, chat rooms, and web links for forms and feedback[7].
4. **Logic Bombs**- A logic bomb is a type of code purposely introduced into a software program that would set off a destructive operation when requirements are met. E.g., a programmer can hide a piece of code that keeps deleting files from the database of a company. A logic bomb is a malicious code that attackers inject into a program or operating system. This code remains latent until a situation arises. Such conditions may be a fixed time or a particular command the user inputs in. When situations arise, the logic bomb can destroy the operating device (corrupting the hard disk, stealing records, or overtaking the computer). Hackers also use logic bombs of viruses, worms, and Trojan horses to do optimum damage. Indeed, when used as a logic device, certain forms of malware can behave in one manner and radically shift tactics until the conditional requirement is reached[1].

5. **Virus Dissemination**. Viruses are computer programs that infect or corrupt a device or data and appear to circulate on a network among other devices. They interrupt the system process and damage the storage data, either by changing it or totally removing it. Virus propagation is a destructive malware mechanism connected to certain applications. Virus, spiders, Trojan Horse, Logic Bomb, Rabbit, and Bacterium are instances of malware that breaks the victim's machine. Some Trojan generation tools enable hackers to construct their own Trojans. These toolkits help hackers develop personalized Trojans. These techniques can be risky and backfire if not properly executed. New Trojans produced by hackers typically have the added benefit of going undetected by virus detection and Trojan scanning tools because they don't suit any known signatures. Viruses and worms can be used to manipulate software to allow an intruder to gain access. A virus and a worm are similar; both being a form of malicious software (malware). A virus infects another program and uses it to spread itself. The virus code is inserted into the already safe software and shows its effect while operating the application[8].
6. **Phishing-** Phishing is a cybercrime in which an attacker acting as a legitimate institution contacts to target via an e-mail, telephone, or text message for the purpose of enticing individuals to provide confidential information such as personally identifying information, credit card details, and passwords. The details are then used to access valuable accounts, contributing to data fraud and financial damage. The first phishing case was brought in 2004 against a Californian youth who developed an "America Online" replica website. Using this fake website, he was able to obtain confidential user information and use credit card details to withdraw money from their accounts. Aside from email and website phishing, there are also 'vishing' (voice phishing), 'smishing' (SMS Phishing), and many other cybercriminal phishing tactics[9,10].
7. **The Denial of Service attack (DoS)-** DoS is a type of cyber assault, in which an attacker attempts to disrupt a computer or any device by interrupting the usual operation of the software to its intended users. DoS attacks typically work by flooding a specific system with requests until regular traffic is not handled, which contributes to device denial of service. A DoS assault is characterized by the usage of a single device to attack the target. A DoS assault is specifically aimed at over-saturating the ability of a specified system, leading to subsequent requests being denied[11,12].
8. **Email Bombing-** Email bombing is characterized by an attacker sending a large number of emails to a target address leading to the crashing of the victim's email account or mail servers. The email is irrelevant and too lengthy for network resources to be absorbed. When several mail accounts are targeted, they may have a denial-of-service effect[13].
9. **Web Jacking-** Web jacking means seeking control over the website of victims. it is simple if someone clones your website and trick you to assume that the cloned site is yours. The malicious link is on your website, waiting for a click. when that link is clicked it is replaced by a malicious web server. It is very different from the normal forms of phishing. Normally, if anyone wants to hijack a Website, the name on the address bar subtly shifts from your original website when the victim clicks on the link. E.g., if the original is www.cyber.com, something like www.ciber.com or something quite similar might be visible[14].
10. **Identity Theft and Credit card frauds-** Theft of identity and credit card frauds- Identity theft occurs if a person steals a victim's identity to claims that he has access to resources such as credit cards, bank accounts, and other benefits in the victim's name. The impostor can use the victim's identity to commit other crimes as well. Credit card fraud is a broad term for identity theft crimes where the criminal uses someone's credit card to finance his or her operations. Credit card fraud is the easiest method of identity theft. The most popular form of credit card theft is the pre-approved card that gets into the possession of someone else[15].

11. **Salami Attack**- A salami attack occurs where minor attacks add up to a large attack that is not detected. This is also known as salami slicing. Although salami slice is frequently used to carry out criminal acts, it just represents a tactic to achieve an edge in time by building up to it in minor increments, so it can be utilized in a perfectly legal manner. One basic illustration is where an attacker deducts Rs. 0.01 (1 paisa) from an SBI account. Nobody would notice such a small flaw. However, if one paisa is deducted from all Indian bank holders, it generates a large amount of money. Computer computations are rounded to small fractions several times. Most banks attempt to rob money when making these corrections[16].
12. **Cyberstalking**- Cyberstalking in our society is a common type of cyber-crime where someone is tracked or followed online. A cyberstalker does not follow his victim physically, he practically does so by following his online activity, collecting information about the stake, and harass the victim. It is a breach of one's online privacy. Often victims are women who are stalked by men and children stalked by paedophiles. Cyberstalkers target their victims by email, chat rooms, directories, forums of conversation, and open websites. The availability of free email/website space and the anonymity of chat rooms and forums have led to an increase in cyberstalking. Everybody has an online profile now so it is very easy to check Google to collect the name, contact number, and address, which leads to the risk of cyberstalks. As the internet is becoming an extremely essential part of our personal and professional lives, stalkers with just a few clicks away can take advantage to obtain information about the victim[17].
13. **Software Piracy**- With the advancement and development of internet websites and torrents, virtually any video, program or song can be found free of charge. Online piracy is an intrinsic aspect of our existence, to which we all lead intentionally or unintentionally. This affects the income of resource developers. It's not only about exploiting the intellectual property of anyone else illegally but even handing it over to your mates to reduce their profits. Computer piracy is illegal electronic program use and delivery. Software developers work hard to develop such services and piracy curbs their capacity to produce adequate money to fund the creation of software. It affects the world economy when revenues are diverted from other markets, resulting in less advertisement and analysis spending. software piracy includes installation up the PC with unlicensed software, use of single-licensed software on many computers, use a key generator to disable copy security, distribution of the cracked version of software online and offline[18,19].

Emerging trends of Cyber-crime in Jammu and Kashmir

For our daily lives, computers and the Internet are becoming relevant. About 1,00,000 persons worldwide had internet access in 1990. There are now approximately 4.57 billion internet users worldwide according to the STATISTA report. Improved and increased use of Information technology gives ordinary people to access, store, and share information across the globe. The cyber-world is a digital world wherein a person is able to perform his personal acts as easily and freely as possible, and the online world serves as the platform for all electronic services and practices. The primary mode of data exchange in the present world is e-mail and websites. This includes not only instructional and informational material but also personal information. India has the 2nd largest internet user after China, with a surge of 564.5 million internet users in the year 2020 (figure1). Facebook users worldwide overtook the United States and for the first time, India has provided a growing consumer network[20]. The 20th century has brought to life the concept of a global village, with digital technology interconnecting and intertwining the markets, societies, and communities of the planet. India is no different, with over 400 million internet users as of 2018, making it the second-largest internet population in the world and each year internet crimes are touching its skys (figure.2). Although accessibility across the world wide web is promising significant change, it also throws up new threats to our digital communities. Cybercrimes know no bounds and

are developing at the same pace as new technology. The insertion of mobile networking and expansion of the GPRS system in the erstwhile state of Jammu and Kashmir has developed new mass rhetoric since 2003. The swift advancement of the telecom services blended with the infusion of rapidly growing private networking in Kashmir derived people towards a more advanced type of connectivity. The number of mobile/landline network connections per 100 people in a particular zone or area (teledensity) was found be to 53.22% in 2012 with an estimated number of about 6.1 million network connections (Mobile). The statistics documented by Telecom Regulatory Authority of India (TRAI) in 2015 a teledensity of 79.5% with mobile users of about 9.6 million with netizens touching the figures of 3.5 million. Just by a year or so the subscriber's number reaching about 117 million and a teledensity of 94.34% in 2017 which kept on growing rapidly[21]. There is a dramatic rise in cybercrime in Jammu and Kashmir, with 73 such crimes reported in the state in 2019. Official figures of the National Crime Records Bureau (NCRB) indicate 73 and 63 cyber-related crimes in Jammu and Kashmir have been observed in 2018 and 2017 respectively. According to figures, 38 cybercrime incidents were registered in 2015, while 25 were registered in 2016 (figure.3). In collaboration with the State Department of Finances and house government, the proposal to alert cyber-crime police stations and the workplace's growth was under consideration recently. most police stations are provided with new IT gadgets/ technology designed to efficiently combat cyber-crimes[22]. The latest victim of cyber-attack in J&K was on servers of the state power department where Hackers removed critical information from servers, pushed their engineers into a frenzy situation. However, the attack was then defended and data was backed up by the authorities[23]. Another well-known cyber-attack was carried on the National Institute of Technology (NIT) Srinagar in June 2017 where a group of hackers hacked the NIT website and posted anti-India messages on the website[22]. Following the case, some spam on the online sale of refurnished goods at a much lower price was circulating across the OLX and Facebook accounts, which were stated to be diligent and cautious by J&K cyber cell. "Any customer who has an interest in purchasing the item posted by the fraudsters were made to believe that they serve in the military or other defence agency and selling products to a lower price due to their transfer, thereby rendering innocent and unaware of transferring the sum to their e-wallets/bank accounts and eventually deceiving and getting the money from innocent people. With this regard, the Cyber Police of J&K rescued Rs130,000 from fraudsters and also blocked numerous counterfeit bank accounts used in the crime commission[24].

There are few instances of the way that social media in recent times have been misused and have been a source of false rumours. Many of these stories were circulated by anonymous profiles. This is at a time when the world is trying to combat the latest coronavirus pandemic, and many people rely on social media to improve their safety and stay updated about the pandemic. Administrative agencies, doctors, and journalists often use social media to share new information to stay updated with the safety measures and precautions about the disease.

Several media channels became a victim of false information. For example, many news portals displayed the fake NEWS of the 4G internet order of the Supreme Court. The Cyber Crime Division of J&K has reported nine cases of abuse of social media since the coronavirus outbreak and at least 178 people in the valley were arrested after fake news, videos, and pictures were posted[25]. Cyber Police in Srinagar, Jammu Kashmir has set up its response team and stepped up efforts to tackle cybercrimes in the Valley. Such action came into effect after a string of complaints received by the police through different channels that certain people were using false identities in social media to abuse women. In certain cases, men were using morphing photos and threatening women. There are a few instances where several women were not willing to make official complaints, fearing shame and embracement. however, The J&K Cyber Crime Team has time to encouraged such victims to come forward against cyber-crime and ensured that their identities would remain confidential[26].

Cybercrime in J&K also involves problems relating to the setting up of fake Facebook accounts, fake online profiles, or unauthorized access to another person's account through fake identity, with the aim of cheating. The Cyber-crime wing of J&K Police also

seized lakhs of rupees from the hackers disguising themselves as bank representatives and online business operators to target people for financial crimes. The anti-corruption bureau (ACB) arrested the accused in Jammu and Kashmir Co-operative Bank in a huge scam Rs. 223 crore which emerged in March 2020[27]. Following a six-month inquiry into incidents of violence in Kashmir in 2017, a team of the National Investigation Agency (NIA) found 79 WhatsApp groups, with 6,386 phone numbers, used to scoop up stone-pelting boys. Of these, about 1,000 active numbers were identified from Pakistan or the Gulf States. In different areas of the Valley and neighbouring states, the remaining 5.386 numbers were found involved. Most of these groups had Pakistan-based administrators[28]. In Kashmir, the number of young people with free access to social media grew from 25% in 2010 to more than 70% in 2015. Since then it can reasonably be concluded that this number has risen. In 2016, the Government for the first time took action by banning internet communications for five months to control violence and terrorism. Online curfews typically suspend 3G and 4G networks and social media services[29]

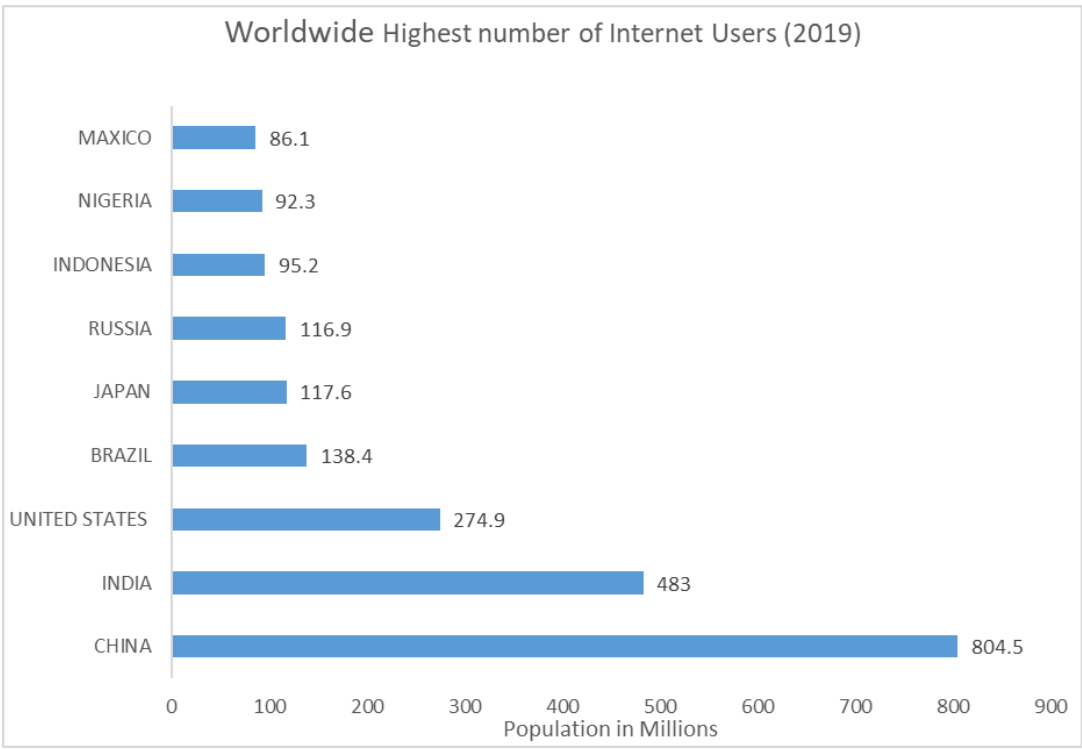

Figure 1: Countries with the highest number of internet users worldwide

Social media is proving to be a potent tool for militant groups in today's times. Earlier they had to strive for reaching out to the people through newspaper columns and audio messages on the radio. However, social media has provided them with an easily accessible platform that enhances their outreach. The social sites are filled with posters, pictures, and messages of different individuals and organizations associated with the different outfits. The content is diffused into the world faster than the air via encrypted means like WhatsApp, telegram, etc. The sloganeering near encounter sites, recording of militant's family phone calls, training videos of militant groups, the self-styled photography displaying arms and ammunition have been considered as acts of charisma by the youth in Kashmir[30].

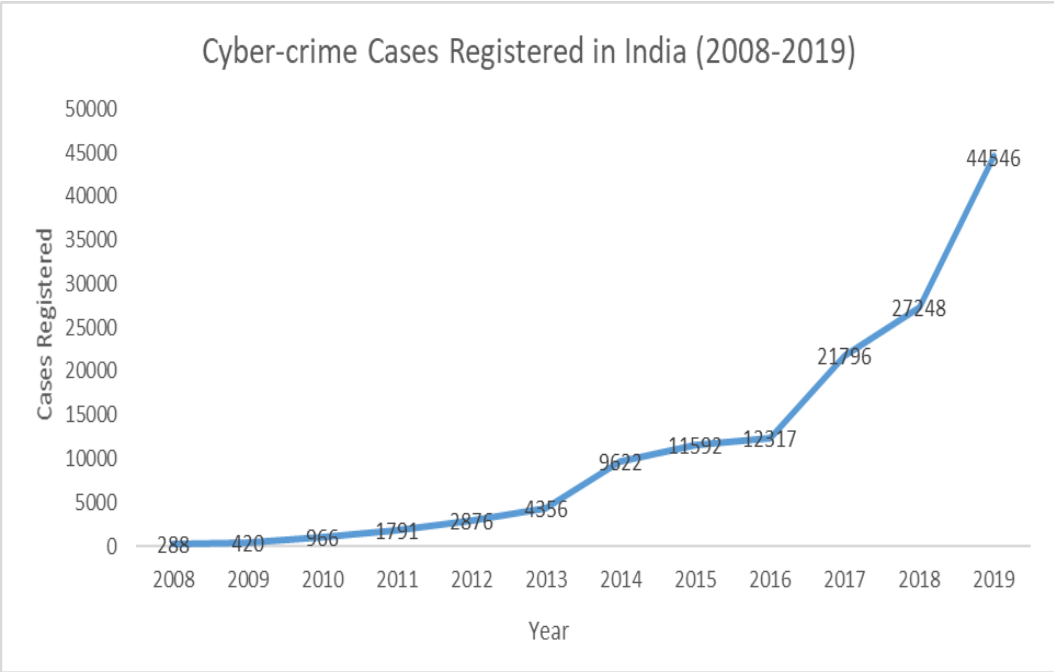

Figure 2: Cybercrime cases Registered in India (2008-2019.

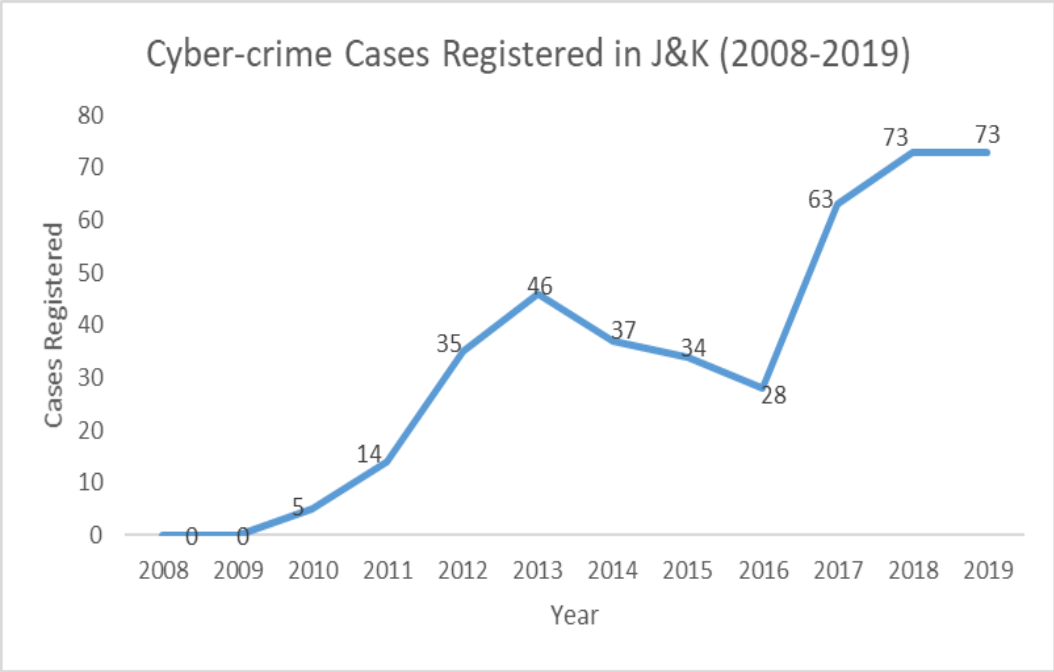

Figure 3: Cybercrime cases registered in Jammu and Kashmir (2008-019)

The rebirth of agitation and mass demonstrations has ensued in correspondence with the rapidly growing number of netizens in the last decade. The mass agitation of 2008 was largely influenced the get together of protesters. The footage of the protesters diffused through the internet to the nook and corner of Kashmir captivated protesters towards the agitation. Although, the separatist groups alongside the enraged protesters used this platform in 2010 more extensively so as to mobilize more masses. The more entanglement of mobile users towards social media sites has led to a model shift with regard

to the protests and protesters. The alteration has been swayed by the control and restrictions on the conventional media houses. During the 2010 uprising, the government came heavily on the mainstream media lines and stopped some newspapers, and curtailed the printing process of many publishers. Some of the channels that reported from ground zero and covered the stories related to agitation were also restricted and banned in the context of provocation of violence This hardened censorship on the news sources compressed the conventional media thus made way for the alternative media sources. Adding to the list of restrictions the government at the same time imposed a ban on SMS services as well in the context of law and order. The ban lasted for about four years and was abrogated in May 2014[21]. After the 2016 unrest in Kashmir, the Government banned various social media sites in the context of law and order. The websites that are banned include YouTube, Telegram, QQ, WeChat, Tumblr, Viber, Reddit, and Flickr. The ban was lifted after the situations were under control, however, since then there were many incidents where the government banned mobile services, social media sites, and/or internet services[31].

Role of Law Enforcement to Tackle Cybercrime in J&K

In the combat against the terror in the newly created union territory, the Jammu and Kashmir (J&K) police are at the forefront, but modern challenges are still present. Kashmir has contended with a lot of false propaganda on websites of social networking, which are being deeply tracked by cyber cells. A lot of this form of social networking propaganda is rooted in Pakistan. The internet was shut down in the valley after the revocation of Article 370 and this led to a variety of propaganda profiles from across the border. Although the action for the establishment of law and order was taken in numerous cases in the valley, the security forces performed well. After the encounters, videos from sites were made viral and people were invited to gather near locations, which have now stopped entirely. Many individuals were arrested and no other events have happened thereafter. Stone Pelting was also a big challenge for security forces. Several WhatsApp groups were used to gather stone-pelters from various locations. The cyber cells have shut down hundreds of WhatsApp groups that are actively involved in these events. In Srinagar, the cyber laboratories are keeping eyes on miscreant social media handlers. IT experts and digital forensic units along with the crime branch of Srinagar are tracking and monitoring cyber crimes. Cybercrime has proven to be a major problem for law enforcement officials in the valley. Cyber teams have done everything possible to combat and hold propaganda content to inspire young people[32].

Conclusion

The immense rise in Internet usage in the world and particularly in India has led to India becoming vulnerable to such crime. Cybercrimes are worldwide and offenders are not related to a single geographical region. Cyberspace is free-flowing, unbounded, and not covered by local regional restrictions. The current way of living has been transformed by new technology. The internet has given us many advantages. Whether connecting with friends, seek information, do financial transfers, access online resources, find a career, find a life partner, or even run whole companies. internet is a basic need. Nearly all facets of our lives come from the Internet. It is often vulnerable for users to a wide variety of attacks. The internet is constantly targeted by new and strong cyber threats. Slight error management of our online life will unlock the gates for cybercriminals. they can steal victim's money or ruin their reputation. Online fraud and cyberspace abuse are rampant around the world, and in Kashmir, users are not immune to such risks. In the Cashmere Cyber Police Station of Srinagar, several complaints about the exploitation of cyber-space are received, mainly online financial fraud. To cheat/hide the gullible people, cyber fraudsters and scammers continue to change their way of operating. Cyber police Kashmir is actively recommending to the general public to be highly vigilant, not to be exposed to numerous cybercrime frauds such as unexpected prizes or rewards, jobs offerings, the construction of cell phone tower offers, loan offers, insurance incentive offers, etc. and not to exchange bank details /personal information or transfer funds to unknown people. Cyber Police of Kashmir has always encouraged people to stay away from e-crimes and advises people to promptly report such incidents.

Declaration of Conflicting Interests: The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding: The author received no financial support for the research, authorship, and/or publication of this article

Ethical clearance: Not applicable

References

1. Dashora K, Patel P. Cyber Crime in the Society: Problems and Preventions. Vol. 3, Journal of Alternative Perspectives in the Social Sciences. 2011.
2. Kandpal V, Singh RK. Latest Face of Cybercrime and Its Prevention In India. Artic Int J Sci Basic Appl Res. 2013;2(4):150–6.
3. Jahankhani H, Al-Nemrat A, Hosseinian-Far A. Cybercrime classification and characteristics. In: Cyber Crime and Cyber Terrorism Investigator's Handbook. Elsevier Inc.; 2014. p. 149–64.
4. Yar M. Computer Hacking: Just Another Case of Juvenile Delinquency? Howard J Crim Justice. 2005 Sep 1;44(4):387–99.
5. Zhang X, Tsang A, Yue WT, Chau M. The classification of hackers by knowledge exchange behaviors. Inf Syst Front. 2015 Dec 1;17(6):1239–51.
6. Ali NS, Shibghatullah AS, Al Attar MH. Review of the defensive approaches for structured query language injection attacks and their countermeasures. J Theor Appl Inf Technol. 2015;20(2).
7. Hydara I, Sultan ABM, Zulzalil H, Admodisastro N. Current state of research on cross-site scripting (XSS) - A systematic literature review. Vol. 58, Information and Software Technology. Elsevier B.V.; 2015. p. 170–86.
8. Brenner SW, Schwerha JJ. Introduction - Cybercrime: A note on international issues. Vol. 6, Information Systems Frontiers. Springer Netherlands; 2004. p. 111–4.
9. Konradt C, Schilling A, Werners B. Phishing: An economic analysis of cybercrime perpetrators. Comput Secur. 2016 May 1;58:39–46.
10. Younis YA, Musbah M. A framework to protect against phishing attacks. In: ACM International Conference Proceeding Series. Association for Computing Machinery; 2020.
11. Carl G, Kesidis G, Brooks RR, Rai S. Denial-of-service attack-detection techniques. IEEE Internet Comput. 2006 Jan;10(1):82–9.
12. Moore D, Shannon C, Brown DJ, Voelker GM, Savage S. Inferring internet denial-of-service activity. ACM Trans Comput Syst. 2006;24(2):115–39.
13. Adeyinka O. Internet attack methods and internet security technology. In: Proceedings - 2nd Asia International Conference on Modelling and Simulation, AMS 2008. 2008. p. 77–82.
14. Razzaq A, Hur A, Ahmad HF, Masood M. Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. In: Proceedings - 2013 11th International Symposium on Autonomous Decentralized Systems, ISADS 2013. Institute of Electrical and Electronics Engineers Inc.; 2013.
15. Kahn CM, Roberds W. Credit and identity theft. J Monet Econ. 2008 Mar 1;55(2):251–64.
16. Alhassan NS, Karmanje AR, Yusuf MO, Alam M. Salami Attacks and their Mitigation-An Overview. Proceedings of the 12 th INDIACom; INDIACom. 2018.
17. Pittaro ML. Michael Pittaro-Cyber stalking: An Analysis of Online Harassment and Intimidation Cyber stalking: An Analysis of Online Harassment and Intimidation. Vol. 1, Cyber Criminology (IJCC). 2007.
18. Reavis Conner K, Rumelt RP. Software Piracy: An Analysis of Protection Strategies. Manag Sci. 1991 Feb 1;37(2):125–39.
19. Fernández-Márquez CM, Vázquez FJ, Watt R. Social influence on software piracy. Manag Decis Econ. 2020 Oct 1;41(7):1211–24.
20. Sandhya Keelery. Internet usage in India - statistics & facts | Statista [Internet]. statista. 2020 [cited 2020 Dec 5]. Available from: https://www.statista.com/topics/2157/internet-usage-in-india/
21. Nadaf AH. Digital Dissent and Censorship in the Kashmir Conflict. In: Platforms, Protests, and the Challenge of Networked Democracy. Springer International Publishing; 2020. p. 293–312.
22. Gupta A. A Study on Cybercrime in Jammu & Kashmir. Int J Res Appl Sci Eng Technol. 2018 Feb 28;6(2):595–8.
23. Hackers target J&K Power Development Dept, wipe out essential data, IT News, ET CIO. Economic T1mes. 2020 Jun 27;
24. Yaqoob M. Cyber police issue advisory as online fraud complaints galore | Greater Kashmir. Greter Kashmir. 2020 Jul 23;

25. Kuloo M. Jammu and Kashmir Police struggles to combat fake news on coronavirus outbreak and internet restrictions; 178 people arrested in Valley - India News , Firstpost. First Post. 2020 Apr 22;
26. Top cops to devise mechanism to deal with cyber crime cases | Greater Kashmir. greater kashmir. 2020 Jun 25;
27. Awasthi P. Cyber police in Kashmir gears up taskforce to curb online crime - The Hindu BusinessLine. 2020 May 20;
28. Bhatia V. WhatsApp used to gather stone pelters, many admins abroad: NIA | India News,The Indian Express [Internet]. The India Express. 2017 [cited 2020 Dec 27]. Available from: https://indianexpress.com/article/india/whatsapp-used-to-gather-stone-pelters-many-admins-abroad-nia-4828984/
29. Bbhatt parjanya. Cyber Jihad: The biggest challenge in Kashmir | ORF [Internet]. 2019 [cited 2020 Jul 31]. Available from: https://www.orfonline.org/expert-speak/42391-cyber-jihad-biggest-challenge-kashmir/
30. Shah khalid. Why Kashmir's new militancy is harder to defeat than the one in 1990s. The Print. 2020 Jan 11;
31. Irfan H. Social media: J&K government bans social media in Valley - The Economic Times. Economic times. 2017 Apr 27;
32. Mir M. J&K police cyber cell bursts terrorists fake propaganda social media | India News – India TV. India TV. 2020 Oct 1.