Cyber Crime-Diffusion, Effects, and Framework towards More Secure Cyber Security Network Governance in India

'What is illegal offline is illegal online'

Venkat Ram Reddy Minampati*
Jyoti Singh

Connectivity and Cyber Crime Diffusion

The use of computers and other information communications technology (ICT) has changed the "traditional" types of crimes and its reach, with risks extending to many aspects of social life, including financial transactions, sexual offences, harassment and threat of attack, commercial property damage, and disorder. The terms "cybercrime" and "cyber-enabled crime" are used to refer to two different but connected criminal actions. Cyber-criminals have access to opportunities online. Cyber-dependent crimes are those that require the use of a computer, computer systems, or similar ICT. This includes the dissemination of viruses and other malicious software, hacking, and the traffic overload of internet servers. The majority of cybercrimes involve attacks on computers or network resources, while they can also have unintended consequences like scam, forgery etc. Traditional crimes that are made more serious or ubiquitous by the use of computers, computer networks, or other ICT are referred to as "cyber-enabled crimes". Unlike crimes that depend on ICT, these can still be perpetrated without it. Fraud encompassing e-commerce, online banking, phishing emails, and other email scams. Grooming and the ownership, fabrication, and/or spread of sexual imagery are examples of sexual offences against children. Theft, including data connected to identification and personal information.

Intelligent, adaptable competitors now occupy cyberspace as a playing field. Attackers and defenders compete in cybercrime races while alternately creating new countermeasures to one another's efforts. The cybercrimes take place across a variety of cyberspaces, including networks that are subject to Denial-of-service assaults, corrupted enterprise systems that are

* **Venkat Ram Reddy Minampati** is an Associate Professor of Public Administration at the School of Liberal Studies, Pandit Deendayal Energy University, Gujarat, India; **Jyoti Singh Raghuvanshi** is a Ph.D Scholar of Public Administration from the School of Liberal Studies, Pandit Deendayal Energy University, Gujarat, India

.

profiled by internal reconnaissance, and anti-virus detectors that come across unexpected malware.

The majority of today's defences are reactive; to stop a new attack, it usually takes identification, a human response, and design intervention. They are insufficient to deal with the size, intensity, and adaptive tactics of harmful parties, all of which are always growing. Moreover, new criminal practices have emerged that aim to compromise the security of computers and its networks, such as proliferation of virus and hacking. Infrastructure and national security are also at risk in addition to people and businesses. Law enforcement is terribly challenging because of the transnational nature of cybercrime, which allows any networks to be targeted from governments all over the world.

Cyber Crime Operations and Offenders (You May Be Next)

We are all impacted by cybercrime, both as individuals and as a nation. On one hand, current technology has facilitated a number of facets of our life, including social connections, banking, shopping, and more. On the other hand, as we depend more on the Internet, there are more dangers and opportunities for illegal activities. Cybercrimes have a variety of motivations. They mostly concentrate on monetary gain and occasionally involve criminal harm or act as a form of protest. There is little doubt that financial gain is not usually the goal of child exploitation. Cybercriminals may be driven by less conventional reasons like intellectual challenge or curiosity, general malice, vengeance, or even just boredom. Offenders may not necessarily need advanced technical knowledge to perpetrate crimes that are enabled or dependent on the internet.

.

Owing to the creation of complex and automated "do-it-yourself" malware kits and hacking tools that are offered for sale on web forums, a larger pool of semi-skilled people now have access to opportunities for complex forms of criminal activity. Yet, cybercrimes go beyond simple technological knowledge and primarily rely on the actions of the targeted victim. To trick computer users into thinking a file or email they have received has a legitimate purpose, social engineering techniques are essential. The majority of the information that has been published regarding cybercriminals has been derived from a small number of case studies or interviews, and it usually focuses on the tactics and driving forces of the offenders. There isn't much thorough published evidence when it comes to other important facts, such as offender traits, career paths, and the links between online and offline crime.

Cyber Crimes in India

It has been noticed that cybercrime has been steadily rising, posing new problems and difficulties for law enforcement agencies. Since cybercrime differs greatly from traditional crime in terms of its nature, breadth, means, evidence, and activities, information transmission in real-time or close to real-time is crucial for the gathering of evidence needed to prosecute cybercriminals. Offenses related to cybercrime are intricately crafted to evade the enforcing agencies both legally and technically. Because cyberspace and cybercrime have no physical limits, international collaboration is essential for investigations, the gathering of data and evidence, and punishment, among other things. With more than 560 million internet users, India is the second-largest online market in the world, only behind China, according to data from the national crime records bureau (NCRB 2021). Also, it is anticipated that by 2023, there will be more than 650 million internet users in the country. In India, there were 27,248 cases of cybercrime reported in 2018. CERT-In statistics revealed a rise in cyberattacks from 41,378 in 2017 to 14,02,809 in 2021. However, in 2022, where 12,67,564 attacks were registered till

.

November, this number seems to have slightly dropped by December. In response to inquiries regarding the country of origin of these assaults, the Ministry of Electronics and Information Technology (MeitY) stated that "the Internet Protocol (IP) addresses of the computers involved in the attacks appear to have come from a number of countries, according to CERT-Investigation."

Legislations and Framework

Legislative actions are crucial in the prevention and eradication of cybercrime. They are necessary in all contexts, including criminalization, procedural authority, jurisdiction, intergovernmental collaboration, and accountability and responsibility of internet service providers. Cybercrime laws at the national level, whether they are already in place or are being drafted, frequently deal with criminalization, showing an emphasis on creating specialised offences for key cybercrimes. But nations are becoming more aware of the necessity for legislation in other fields. The current laws and upcoming cybercrime legislation more typically cover investigation techniques, jurisdiction, electronic evidence, and international collaboration. The Information Technology Act 2000, as revised in 2008, and the Indian Criminal Code served as India's national legislative and institutional framework for dealing with cybercrime, providing the legal framework to address e-commerce, cybersecurity, cybercrime, and cyberterrorism. Most matters relating to cybercrime are covered under the country's broad legislation. A draft national cyber security strategy that takes a comprehensive approach to addressing the issue of national cyberspace security has been developed by the National Security Council Secretariat (NSCS). The CERT-In organisation frequently releases alerts and advisories on the most recent cyber threats, vulnerabilities, and security precautions for networks and systems. The Ministry of Home Affairs' (MHA) Indian Cyber Crime Coordination Centre (I4C) has been appointed as the focal point for the fight against cybercrime.

International Cooperation

In accordance with United Nations General Assembly resolution 75/282, which was adopted in May 2021, all the member nations formed an ad hoc working group to develop a "Comprehensive International Convention on Countering the Use of Information and Communications Technology for Criminal Purposes." India, a committee member, has

.

suggested that the stated Convention make cyberterrorism a crime. The Ministry of Home Affairs has released the Central Ministries, State governments, and their Policy and Guidelines to prevent information security breaches and cyber intrusions in the information and communication technology infrastructure.

India is one of Interpol's founding members. An institution like Interpol is absolutely essential for cooperation and multilateralism in the modern world. In order to create cross-sector alliances and enable global law enforcement cooperation, close cooperation between INTERPOL and its global reach is essential. In order to lessen cyber risks, INTERPOL organises law enforcement operations and provides secure data exchange platforms, analysis, and training. INTERPOL can assist in securing communities for a safer world by utilising the constantly expanding ability of our member nations to stop, detect, investigate, and disrupt cybercrimes.

Electronic Evidence and Criminal Justice

The establishment of facts pertaining to a person's guilt or innocence at trial is done through the use of evidence. All such digital or electronic evidence is referred to as electronic evidence. Electronic evidence is becoming more and more important in criminal cases overall as well as in the investigation and prosecution of cybercrimes. An efficient response to crime therefore requires legal frameworks that are optimised for electronic evidence, as well as law enforcement and criminal justice capabilities to locate, gather, and analyse electronic evidence. Computer- user interaction equipment generates vast number of electronic traces that can be used as evidence. Gigabytes of images, videos, emails, chat logs, and system data could all be potentially relevant to a criminal act, as could other computer data and electronic interactions. It can take a long time to find the pertinent information in this data. Finding the right information is made more difficult by the number of available file formats, operating systems, application software, and hardware specifications. When it comes to digital information, both the tangible objects that contained the data when it was received or seized and the stored data that was present on the device must be kept as continuous pieces of evidence. In order to do so, the source of the evidence must show that, the details that is intended to be accepted as evidence is exactly same as that was initially revealed and then taken into custody.

.

Digital Forensics

The recovery and evaluation of information found in digital and computer systems is the focus of the branch of forensic science known as "digital forensics." Information kept on electronic devices, such as computers and cell phones, is brittle and is easily changed or tampered with during investigations. Yet, it is simple to replicate such data. Creating a replica of the storage device or an undisturbed forensic picture, which has the most accurate representation of the original device as is possible, is consequently a critical initial step in many digital forensics' investigations.

Every efficient and successful government system relies on the justice system to keep criminals under control. Justice is what makes sure that society has good government. If justice is alert at all times, it is then only that citizens and society remain brave, and a healthy society is established. The National Forensic Science University (NFSU) was recently established, among other innovative measures the Indian government has lately made to address upcoming difficulties. The 'Crime and Criminal Tracking Network and System' is being linked with the fundamental elements of criminal justice, including e-Courts, e-Prison, e-Forensics, and e-Prosecution, under the name of I.C.J.S. (CCTNS). A national database on crimes like terrorism, narcotics trafficking, and white collar crimes would also be created, according to the Indian government. Indian Cyber-Crime Coordination Centre (I-4C) was formed by the Indian Government as a comprehensive response system against cybercrime.

Cyber Crime Prevention

The term "crime prevention" refers to methods for limiting the many factors that contribute to criminal activity in order to lessen the likelihood that crimes will occur and the potential harm they may cause to both persons and society. The principles of the United Nations for crime prevention focuses on the importance of government leadership, as well as cooperation and partnerships between departments and agencies, local organisations, non-governmental organisations, the corporate community, and private citizens. Crime prevention is particularly difficult when it comes to cybercrime. The comparative openness of people to engaging in "risky" online behaviour, the potential for anonymity and deception strategies on the part of offenders, the multinational aspect of many cybercrime actions, and the rapid speed of criminal

.

innovation are a few of these factors. The organisation, strategies, and tactics used to prevent cybercrime are affected by each of these difficulties. Organizational structures must take into account the requirement for regional and international cooperation in combating cybercrime. A variety of stakeholders, especially in the corporate world who maintain and control the internet's infrastructure and services, will need to be involved in methods and techniques to maintain a continually updated picture of cyber dangers.

The government has created a platform, the National Cyber Crime Reporting Portal (www.cybercrime.gov.in) for the general public to notify instances of any kind of cybercrime, with a focus on crimes against women and children. The ministry of Home affairs recently developed 'Digital Police' portal at national level to register the cybercrime and integrated citizen services (concerned with police department) for an easy accessibility. Under the national cyber–Crime Reporting Portal, all the services specific to woman and children have been placed for reporting openly and anonymously. Tracking the cyber complaints were made digital. Novel idea of creating Cyber Crime Volunteers to report the unlawful content uploaded by criminals and report the same to the appropriate authorities. And encouraged individuals also to volunteering. A toll-free number '1930' has been operationalized for assistance in filing online cybercrime complaints. Also, a module of the Citizen Financial Cyber Fraud Reporting and Management System was launched to allow the quick reporting of financial frauds which will prevent money from being stolen by attackers. To increase public knowledge of information security, the Ministry of Electronics and Information Technology (MeitY) undertakes various campaigns via websites, "www.infosecawareness.in" and "www.csk.gov.in," specific books, movies, and online resources are created for kids, parents, government employees, teachers, police, family and general users regarding information security.

NOTES

1. UN Global Programme on Cyber Crime, 2013.
2. Dr. Mike McGuire, Samantha Dowling. Cyber-crime: A review of the evidence October2013.
3. Interpol Awareness Campaigns, (Accessed on 2023) www.interpol.in
4. Nidhi Narnolia, Cyber Crimes in India: An Overview, October 2021.
5. Nikunj Arora, Cyber Crime Laws in India, blog ippleaders.in April 2022.
6. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.May 2021.

.

7. http://www.pib.gov.in (Release ID: 1869983) October 2021.
8. General information on do's and don'ts while using cyberspace. www.infosecawareness.in
9. National Cybercrime Reporting Portal. www.cybercrime.gov.in

.