Page 2101 - 2117 **DOI:** *https://doij.org/10.10000/IJLMH.119794*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

Cybercrime Investigation: Panorama, Challenges and Solutions

SHREYA JASORIA[1]

ABSTRACT

Cybercrime is deeply ingrained in the present era and is not a new danger. Cyber technologies create a new paradigm for the criminal, enabling them to commit crime without leaving any traces of evidence behind them. Policing cybercrime has become a herculean task because of the all-pervasive nature of the Internet and the definition of crime being national in nature. There exist a number of Principal Interest groups which constitute nodes of Internet Governance. The role of the public police has to be understood within the light of the informal architecture of Internet Policing. It will help one to understand the vast range of cross-jurisdictional and cross-sectoral impediments which police have to face in order to fully participate in the policing of Internet. The only two digital leads available to the Investigating Authorities are- Internet Protocol Address and Online Digital Handles. In order to understand the intricacies of these leads, the police officials require special training. The investigation procedure is further disturbed by other impediments like lack of reporting of cybercrimes, surveillance and privacy concerns, encryption, search and seizure issues and anonymity and attribution problems.

Keywords: *Cybercrime, Digital Leads, Policing Cybercrime, Cybercrime Investigation.*

I. INTRODUCTION

Cybercrime can no longer be seen as a new danger because it is now deeply ingrained in criminal organizations, significantly influences ordinary crime, and is constantly present. The instruments, strategies, and frameworks that criminal syndicates employ to accomplish their goals have changed.

Cyber technologies create a new paradigm for the criminal—a more sophisticated method to attack the vulnerable—and a new fear for the victim. No longer is the evidence of the perpetrator visible to their victim. Society's adaptation to the ever-increasing world of technology provides unlimited potential for convenience, choice, speed and customer satisfaction in the retail world, but it provides law enforcement with exponentially greater challenges when it comes to ensuring the integrity and safety of that online experience.[2]

[1] Author is a Research Scholar at Faculty of Law, Banaras Hindu University, Varanasi, U.P., India.

[2] Calcum Jeffray & Tobias Feakin, *Underground Web: Cybercrime challenge*, Australian Strategic Policy

 [ISSN 2581-5369]

Modern cybercrime draws no distinction between government targets, larger corporations and individual users. Its sole purpose is to exploit vulnerabilities for gain. Despite calls for law enforcement to 'do more' to prevent and investigate cybercrime, the agencies involved are often hampered in acting due to jurisdictional issues or the complexities of the investigation.[3]

II. POLICING CYBERCRIME

The increasing pervasiveness of the Internet, along with its global, transformative impacts create a range of entirely new demands upon the public police which question their traditional local dominance over the security domain and could in fact marginalise them completely.[4] Not only does the concept of cybercrime produce problems for the police because Internet-related offending takes place within a global context whereas crime tends to be nationally defined, but policing the Internet is also a complex affair by the very nature of policing and security being networked and nodal.[5] While the application of concepts of networked and nodal security may be disputed in the terrestrial world,[6] nowhere is it more networked and nodal than in cyberspace.

A. Cybercrime as the Focus of Policing Cyberspace:

Informational, networked, and globalised transformation of deviant or criminal behaviour by networked technologies contribute to the reorganisation of the division of criminal labour, on the one hand automating and deskilling it,[7] while on the other hand 'reskilling' and empowering the 'single agent' who can single-handedly control a complete and complex criminal activity[8].

If Internet transformations are the key to understanding cybercrime, then in order to understand their impact it is necessary to consider what happens if the Internet is removed from the equation. By applying a simple 'transformation test,' three different groups of cyber-criminal opportunity can be identified as points on a spectrum.[9]

Institute (Jan. 26, 2024, 10:12 AM), https://ad-aspi.s3.ap-southeast-2.amazonaws.com/import/SR77_Underground_web_cybercrime.pdf?VersionId=awHWbEd8jXq47M7awzQ1AQCjDePZdhsY.

[3] *Id.* at 2.

[4] David S. Wall, *Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace*, 8 Police Practice And Research: An International Journal 183, 183-205 (Jun. 25, 2024, 12:35 PM), https://cyberdialogue.ca/wp-content/uploads/2011/03/David-Wall-Policing-CyberCrimes.pdf.

[5] L. JOHNSTON & C. SHEARING, *GOVERNING SECURITY, EXPLORATIONS IN POLICING AND JUSTICE*, (Routledge 2003).

[6] A. Crawford & S. Lister, *Policing,* 27(3) AN INTERNATIONAL JOURNAL OF POLICE STRATEGIES & MANAGEMENT, 426 (2004).

[7] H. Braverman, *Labour and Monopoly Capital*, MONTHLY REVIEW PRESS (1976).

[8] K. Pease, *Crime and the Internet*, Crime Futures an foresight in D.S. Wall (Ed.), 24 (2001).

[9] WALL, *supra* note 3, at 186.

 [ISSN 2581-5369]

At the near end of the spectrum are actions that, while often labelled as cybercrimes, are actually first-generation "traditional" crimes where computers are utilized to communicate or obtain information in order to help plan a crime.

The "hybrid" cybercrimes fall somewhere in the middle of the spectrum. These are "traditional" crimes (such as internationalized frauds and deceptions, as well as the international trade in pornographic materials, including child pornography), for which completely new worldwide opportunities have arisen. However, the third generation of "true" cybercrimes—online intellectual property thefts and spam—are at the extreme end of the spectrum. Since they are the offspring of the Internet, they embody all of its revolutionary traits.[10]

Any legal problems arising tend to relate more to legal procedures than substantive law. The final group, however, are solely the product of the Internet and pose the greater regulatory challenges.[11]

B. Situating the Public Police in the Cyberspace

Internet Policing will help one to understand the vast range of cross-jurisdictional and cross-sectoral impediments which police have to face in order to fully participate in the policing of Internet, by embracing the concept of networking.[12] The Principal Interest Groups which constitute nodes of Internet Governance:

1. Internet Users and User Groups-

Internet users and user groups exert a very potent influence upon online behaviour through censure, usually after the occurrence of ‘signal events’, which are behaviours that may not necessarily constitute a major infraction of criminal law, but nonetheless disrupt the sense of social order.[13]

2. Internet service Providers-

The Internet Service Providers are placed in such a fluid status that even though they are physically located in a specific jurisdiction, they are inclined to function transnationally. The fear of civil sanctions encourages ISP compliance with many of the regulatory demands made of them by the police and other state bodies.[14]

---

[10] *Id*. at 186.
[11] WALL, *supra* note 3, at 188.
[12] B. Dupont, *Security in the age of networks*, 14 POLICING AND SOCIETY 84, (2004).
[13] M. Innes, *Reinventing tradition: Reassurance, neighbourhood security and policing*, 4(2) CRIMINAL JUSTICE, 151–171, 154 (2004).
[14] C.P. WALKER, D. S. WALL & Y. AKDENIZ, THE INTERNET, LAW AND SOCIETY, 3-24, 6.

 [ISSN 2581-5369]

3. Non-Governmental Organisations-

Non-governmental, non-police organisations are a hybrid combination of public and private arrangements that contribute directly to the order-maintenance assemblage by acting as gatekeepers to the other levels of governance, but also contributing towards (cyber) crime prevention.[15]

4. Public Police Organisations-

The role played by the police in policing cybercrimes can vary from force-to-force and investigative tactics usually combine traditional policing methods with the use of computers to investigate wrongdoers and collect evidence, they may also use software-based techniques to proactively police some priority concerns.[16]

Although the public police are located within nation states and work under national laws, they are nevertheless networked by transnational policing organisations, such as Europol and Interpol, whose membership requires formal status as a police force.[17]

The broader governance of the Internet is, thus, characterised by a sense of order resulting from a complex 'assemblage' of networked nodes of security that continually shape virtual behaviour[18], transcend the 'state/non-state binary'[19], and also state sovereignty[20]. Without attributing causality, 'assemblage' describes the relationship between heterogeneous contributors to governance that work together as a 'networked' and functional entity, but do not necessarily have any other unity.[21]

III. DIGITAL LEADS

The digital investigative methods that are used to gather evidence in cases of cybercrimes have their basis in these digital leads-

A. Internet Protocol Address

An Internet Protocol address is a numerical address that is assigned to a computer, which is part of a computer network and makes use of the Internet Protocol to communicate. Internet access providers also assign an IP address to the network device that computers use to access

[15] WALL, *supra* note 3, at 197.
[16] P. Sommer, *The Future for the Policing of Cybercrime*, COMPUTER FRAUD AND SECURITY, 8-12 (2004).
[17] J. SHEPTYCKI, IN SEARCH OF TRANSNATIONAL POLICING: TOWARDS A SOCIOLOGY OF GLOBAL POLICING, Ashgate (2002).
[18] C. Walker & Y. Akdeniz, *The Governance of the Internet in Europe with Special reference to illegal and harmful content*, Criminal Law Review 5, 8 (1998).
[19] B. Dupont, *Security in the age of networks*, 14(1) Policing And Society 76 (2004).
[20] C. Shearing, *Thoughts on sovereignty*, 14(1) Policing And Society 5, 6 (2004).
[21] K. Haggerty & R. Ericson, *The surveillant assemblage*, 51(4) British Journal Of Sociology, 605 (2000).

 [ISSN 2581-5369]

the Internet.[22] The transition from IPv4 to IPv6 is further impacting digital investigations.[23]

If law enforcement officers want to identify a subscriber who has been assigned an IP address by an internet access provider, they can issue a data production order[24] to the Internet Service/Access Provider. To establish a link between (1) the crime, (2) the IP address, and (3) the suspect, the application of additional investigative methods – such as performing a digital forensic analysis of a router distributing the internet connection and interviewing members of the household – may be required. Information that is available on seized computers can also provide law enforcement authorities with further evidence of a crime.[25]

B. Online Handles

An *online handle is* a name an individual uses to interact with other individuals on the Internet. Online handles are a digital lead for three reasons-

1. Allows law enforcement officials to gather publicly available information about an internet user- Publicly available information[26] can be defined as information that anyone can lawfully obtain (a) upon request, (b) through purchase, or (c) observation.[27]

Gathering of publicly available online information as an investigative method is further distinguished into-

i. *Manual gathering of online information*- Information that is publicly available online can be gathered from a wide variety of sources, including: (a) websites open to the general public, (b) social media websites, (c) online phone directories, (d) discussion forums and blogs, (e) news articles, and (f) commercial or scientific reports.[28]

ii. *Automated gathering of publicly available information-*

Certain software like 'Crawler' and 'Spider' software are kinds of software which automatically look for relevant information on the Internet based on certain

[22] WALL, *supra* note 3, at 209.
[23] Rutger Leukfeldt, Snader Veenstra & Wouter Stol, *High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands*, 7(1) International Journal Of Cyber Criminology (May 9, 2025, 8:40 PM) https://www.cybercrimejournal.com/pdf/Leukfeldtetal2013janijcc.pdf.
[24] A data production order mandates that the data custodian provide or make data accessible to law enforcement officials within a predetermined timeframe.
[25] R. Clayton, *Anonymity and Traceability in Cyberspace*, University Of Cambridge (Dec. 24, 2024, 10:04 PM), https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-653.pdf18.
[26] 'Publicly available information' is derived from Article 32(a) of the Convention of Cybercrime and includes information provided by a third party that is only available after registration or payment
[27] Q.A.M. Eijkman & D. Weggemans, *Open source intelligence and privacy dilemmas: Is it time to reassess state accountability?*, Security And Human Rights, 287 (2012).
[28] D.L. Carter, Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies, U.S. Department Of Justice, 285 (2009).

 [ISSN 2581-5369]

parameters, such as certain search terms or images.[29] Automated data collection systems may include advanced options, such as: "plug-ins that enhance the search and analysis capacities of Internet searches, for example, through entity recognition, image-to-image conversion, and automated translation"[30]

iii. Observing online behaviours of individuals-

The observation of an individual's online behaviours can be regarded as the digital equivalent of the investigative method of 'visual observation' in the physical world. the observation of online behaviours concerns *new information that is being generated by individuals*.

2. Can direct law enforcement officials to an online service provider that may hold information about an internet user/ Data Production Orders-

Online handles can also provide a lead to an online service provider that stores information about an individual that may be of interest to law enforcement authorities.[31] Data Production Orders which are issued to the online service providers provide an important piece of evidence in cybercrime investigations. Data production orders that are issued to online service providers can be divided into the following four categories: (1) subscriber data, (2) traffic data, (3) other data, and (4) content data. The categorisation is largely based on the distinctions made with regards to production orders in the Convention on Cybercrime.[32]

3. Can enable law enforcement officials to interact (undercover) with the individual/ Online undercover Investigative Methods-

The distinguishing feature of undercover investigative method is that law enforcement officials *interact* with other individuals – using a fake identity – in order to gather evidence in a criminal investigation.[33] In this context, a fake identity means that they do not reveal that they are law enforcement officials due to which suspects are both unaware of the purpose and the identity of the undercover agents.[34]

---

[29] S. Brinkhoff & A.R. Lodder, *Big Data Mining by the Dutch Police: Criteria for a Future Method of Investigation*, 70, Research Gate (Feb. 11, 2025, 11:11 AM), https://www.researchgate.net/publication/313598065_Big_Data_Data_Mining_by_the_Dutch_Police_Criteria_for_a_Future_Method_of_Investigation.

[30] E.J. Koops, *Police Investigations in internet open sources: Procedural-law issues*, 29 Computer Law And Security Review 654, 655 (2013).

[31] WALL, *supra* note 3, at 213.

[32] Convention on Cybercrime, art. 16-18.

[33] G.T. MARX, UNDERCOVER, POLICE SURVEILLANCE IN AMERICA 11-13 (University of California Press 1988).

[34] E.E. Joh, *Breaking the Law to Enforce It: Undercover Police Participation in Crime*, 61 Stanford Law Review 155, 161 (2009).

With the right knowledge of internet subcultures, law enforcement officials can interact and build relationships with individuals under a credible, fake identity in order to gather evidence in criminal investigations.[35] Further, Online infiltration operations are carried out, which are characterised by the fact that undercover agents are authorised (to a certain extent) to participate in a criminal organisation in order to maintain cover and to gain a targeted individual's trust in a criminal investigation.[36]

IV. IMPEDIMENTS

A. Reporting of Cyber Crimes

Before an investigation begins, a cybercrime must be observed and reported. While this seems like a straightforward first step in a cybercrime investigation, the reality is that cybercrime is largely underreported worldwide.[37]

The underreporting of crime can be explained by economist Gary Becker's (1968) *expected utility theory*, which holds that people engage in actions when the expected utility (i.e., gains) from these actions are higher than the expected utility of engaging in other actions.[38] Applying this theory to cybercrime, victims of cybercrime will not report cybercrimes if the expected utility from this reporting is low.[39]

However, a person or organization's willingness to report cybercrime depends on the type of cybercrime.[40] Existing research identifies several reasons why cybercrime is underreported, including the shame and embarrassment associated with being a victim of certain cybercrimes (e.g., romance scams); reputational risks associated with publicizing cybercrime[41] (e.g., if the victim of the cybercrime is a business, loss of consumer confidence); being unaware that victimization occurred; low confidence or expectations that law enforcement can assist them[42]; too much time and effort to report cybercrime[43]; and lack of awareness on where to report cybercrime.[44]

---

[35] N. Petrashek, *Fourth Amendment and the Brave New World of Online Social Networking*, 9 The Marquette Law Review, 1495, 1528 (2009).
[36] JOH, *supra* note 33 at 166.
[37] Comprehensive Study on Cybercrime- Draft February 2013, (Jun. 28, 2024, 09:26 AM), https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
[38] Marie-Helen Maras, CYBERCRIMINOLOGY, 25 (Oxford University Press, 2016).
[39] *Ibid.*
[40] WALL, *supra* note 3, at 194.
[41] McGuire, Mike and Samantha Dowling, (2013). *Chapter 4: Improving the cybercrime evidence base*, Cybercrime: A review of the evidence. Research Report 75, (Jun. 28, 2024, 02:45 PM) https://assets.publishing.service.gov.uk/media/5a7caa0340f0b65b3de0a624/horr75-chap4.pdf.
[42] M.Levi & D. S. Wall, *Technologies, security and privacy in the post-9/11 European information society*, Journal Of Law And Society, 194(2004).

Since local policing strategies are often reduced to decisions that are made at a very local level over the most efficient expenditure of finite resources[45] the public interest, 'a key criterion in releasing police resources for an investigation, is often hard to justify in individual cases of cybercrime victimisation. This contrast in perceptions is exacerbated by the reassurance gap between what the police and the media perceive as the problem and the signal events[46] that actually shape public perceptions and increase levels of fear of cybercrime. These signal events are in fact often spam-driven small-impact bulk victimisations, or other attempts to victimise online, which increase perceptions of high levels of cybercrime and the dangerousness of the Internet.[47]

B. Surveillance and Interception and Privacy Concerns

The idea of a Panoptikon, of monitoring all communications in India and centrally storing such data is not new. It was first envisioned in 2009, following the 2008 Mumbai terrorist attacks. As such, the Central Monitoring System (CMS) started off as a project run by the Centre for Communication Security Research and Monitoring (CCSRM), along with the Telecom Testing and Security Certification (TTSC) project.

India's Central Monitoring System has been built on lines of Prism, which was in news after Edward Snowden leaked news of global spying to the Guardian and Washington Post. It is an ambitious surveillance system that monitors text messages, social-media engagement and phone calls on landlines and cell phones, among other communications, thereby giving India's security agencies and income tax officials centralized access to the country's telecommunications network. This project, being implemented by the government's Centre for Development of Telematics (C-DOT), is meant to help national law-enforcement agencies save time and avoid manual intervention, according to the Department of Telecommunications' annual report.[48]

---

[43] Maria Tcherni, Andrew Davies, Giza Lopes, and Alan Lizotte. (2016). *The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?* 33(5) *Justice Quarterly*, 890 (Jun. 27, 2024, 04:45 PM) https://digitalcommons.newhaven.edu/cgi/viewcontent.cgi?article=1045&context=criminaljustice-facpubs accessed on 27th June 2024

[44] SOMMER, *supra* Note 15 at 11.

[45] M.Goodman, *Why the police don't care about computer crime*, 10 Harvard Journal of Law and Technology, 645, 686 (1997).

[46] M. Innes, *Reinventing tradition?: Reassurance, neighbourhood security and policing*, 4(2) Criminal Justice, 151 (2004).

[47] WALL, *supra* note 3, at 202

[48] Annual Report 2012-13, Department of Telecommunications, Ministry of Information And Communication Technology, Government of India, New Delhi (Jul. 13, 2024, 5:35 PM) https://dot.gov.in/sites/default/files/Telecom%20Annual%20Report-2012-13%20(English)%20_For%20web%20(1).pdf

 [ISSN 2581-5369]

Prior to the CMS, all service providers in India were required to have Lawful Interception Systems installed at their premises in order to carry out targeted surveillance of individuals by monitoring communications running through their networks. Now, in the CMS era, all TSPs in India are required to integrate Interception Store & Forward (ISF) servers with their pre-existing Lawful Interception Systems. Once ISF servers are installed in the premises of TSPs in India and integrated with Lawful Interception Systems, they are then connected to the Regional Monitoring Centres (RMC) of the CMS.[49]

The surveillance system is not only an "abuse of privacy rights and security-agency overreach," critics say, but also counterproductive in terms of security. In the process of collecting data to monitor criminal activity, the data itself may become a target for terrorists and criminals — a "honeypot," according to Sunil Abraham, executive director of India's Centre for Internet and Society.[50]

1. Privacy under International Human Rights Law:

Cybercrime investigations invariably involve considerations of privacy under international human rights law. Human rights standards specify that laws must be sufficiently clear to give an adequate indication of the circumstances in which authorities are empowered to use an investigative measure, and that adequate and effective guarantees must exist against abuse. When investigations are transnational, divergences in levels of protection, however, give rise to unpredictability regarding foreign law enforcement access to data, and potential jurisdictional gaps in privacy protection regimes.[51]

2. Privacy under Indian Legal System-

Privacy is a necessary condition precedent to the enjoyment of any of the guarantees in Part III. The fundamental right to privacy would cover at least three aspects[52]-

(a) Intrusion with an individual's physical body

(b) Informational Privacy- it protects a person by giving her control over the dissemination of material that is personal to her an disallowing unauthorised use of such information by the State

[49] Maria Xynou, *India's Central Monitoring System: Something To Worry About?*, The Centre For Internet And Society (Jan., 31, 2024, 7:30AM) https://cis-india.org/internet-governance/blog/india-central-monitoring-system-something-to-worry-about.

[50] Anjani Trivedi, P*rism-like Surveillance slips under the Radar,* Time, (Jan., 31, 2024) https://world.time.com/2013/06/30/in-india-prism-like-surveillance-slips-under-the-radar/.

[51] Comprehensive Study on Cybercrime, Draft 2013, xxiiii (May 1, 2024 10:10 PM) https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[52] K.S. Puttaswamy v Union of India, (2019) 1 S.C.C. 1 (India)

(c) Privacy of Choice

In a cybercrime investigation, the use of novel investigative methods, such as CCTV (Closed Circuit Television) cameras or GPS beacons for surveillance purposes, interfere with the Informational Aspect of Right to Privacy.

Both negative and positive obligations emerge from the Right to Privacy. Negative obligations require a State to refrain from interfering with it, unless they can be legitimatised under the conditions stipulated in the Right to Life under Article 21 of the Constitution of India of which Right to Privacy is an integral part. Positive obligations require a State to take the steps necessary to adopt reasonable and suitable measures to protect the rights of the individual.[53] At this time, computers and the Internet play a prominent role in society and creates a platform for crime, against which citizens must be protected. With the duty to protect in this positive sense, States must ensure that domestic law enforcement has the ability to apply the digital investigative methods necessary to an investigation.[54]

C. Encryption

The term 'encryption' refers to the process of converting data from its original form which is in plain text into an indecipherable or scrambled form known as 'cipher text' using a mathematical algorithm. The scrambling of data into cipher text makes it very difficult for the law enforcement officials to read its contents without the key that decrypts data back into the plain original text.

1. Two situations in which Encryption challenges Investigation-

The use of encryption challenges law enforcement officials in Cybercrime investigations-

a. Encryption in Transit- analysis of data in transit

b. Encryption in Storage- when law enforcement officials stumble upon encrypted data on computers during a computer search.[55]

a. *Encryption in Transit*

As a result of encryption in transit, law enforcement officials are often not able to interpret encrypted network traffic that is generated by parties other than internet access providers.[56]

[53] Akandji-Kombe, *Positive Rights under the European Convention on Human Rights*, Human rights handbooks, no. 7, Council of Europe, 7 (2007).
[54] D.S. Wall, *Cybercrime The Transformation of Crime in the Information Age*, 72 (Cambridge: Polity Press, 2007)
[55] R.P. Byrant, *Investigating Digital Crime*, 98 (Wiley-Blackwell 2008).
[56] Internet access providers have to decrypt data that these 'public telecommunication ser- vice- or network providers' encrypt themselves. Many online service providers are not considered as 'public telecommunication

 [ISSN 2581-5369]

This means that the contents of network traffic, such as private messages that are sent over social media services or apps, cannot be read by law enforcement officials.[57]

Wiretaps have historically provided law enforcement officials with useful evidence in criminal investigations but now the law enforcement authorities argue that they are '*going dark*', because their practical ability to intercept electronic communications is declining.[58] There have been certain developments in relation to the use of encryption of data in transit which have challenged the criminal investigation officials.

The first development has been the increase of default encryption implemented by popular online communication service providers. Intercepted communications from these online services are likely no longer readable for law enforcement officials when an internet wiretap is used to gather evidence unless the results of the communications are publicly accessible on the Internet.[59]

The second development is with regard to the increased use of anonymising services that encrypt network data by default. Internet traffic that is routed through VPNs and Tor is encrypted by default, making the data unreadable for law enforcement officials without the keys to decrypt the data.[60]

b. Encryption in Storage

Law enforcement authorities also view the encryption of data in storage as a growing challenge in criminal investigations.[61] Two reasons why encryption in storage has become a major challenge in cybercrime investigations are that encryption is a standard feature in many computers and operation systems and encryption techniques have become easy to use and that.

Full disk encryption on a computer and standard device encryption may leave law enforcement authorities unable to analyse data on a seized computer if they do not obtain the

service- or network providers' or reside on for- eign territory, outside the reach of law enforcement authorities (see Oerlemans 2012, p. 26).

[57] S.M. Bellovin., M. Blaze & S. Clark, & S. Landau, *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12(1) Northwestern Journal Of Technology And Intellectual Property, 1, 12 (2014).

[58] Ellen Nakashima, 'Proliferation of new online communications services poses hurdles for law enforcement', *The Washington Post,* (Mar. 11, 2025, 8:15PM) https://www.washingtonpost.com/world/national-security/proliferation-of-new-online-communications-services-poses-hurdles-for-law-enforcement/2014/07/25/645b13aa-0d21-11e4-b8e5-d0de80767fc2_story.html.

[59] P. Swire, *From real-time intercepts to stored records: why encryption drives the government to seek access to the cloud*, 2(4) International Data Privacy Law, 200-206 (2012).

[60] E.J. Koops, Police investigations in internet open sources: Procedural-law issues', 29(6) *Computer Law and Security Review*, 654 (2013),

[61] S.W. Brenner, *The Fifth Amendment, Cell Phones and Search Incident: A Response to Password Protected*, 96 Iowa Law Review Bulletin, 78, 82 (2011).

encryption key in order to decrypt the data on the computer.[62]

The manual encryption in storage of files 'in the cloud' appears to be a major challenge for law enforcement authorities. These files are unreadable by law enforcement officials, even when they collect the files from third party providers through data production orders.[63]

D. Search & Seizure Issues

'Search' in terms of the Cybercrime Convention implies to seek, read, inspect or review data and it therefore permits both the searching for and the searching or examining of data.[64] Search and seizure of electronic evidence is concerned with data that has been recorded or registered in the past, either in tangible or in intangible form; and the gathering of this data takes place at a single moment in time, in other words, the period of the search, and in respect of data that exists at that time.[65]

The term 'seize' means to take away the physical medium in which data or information is recorded, and includes the use or seizure of computer programs needed to access the data being seized.[66] The seizure of data includes both the gathering of evidence and the confiscation of data.[67]

There is no legislative provision made for expedited preservation of stored computer data. The preservation and disclosure of stored computer data is facilitated by traditional powers of search and seizure. Further, the transborder search and seizure of electronic evidence are facilitated in terms of Mutual Legal Assistance Treaties.[68]

The major problem faced here is that there are only few cyber cells to investigate the matter at the time when the crime rate is doubling. Traditional investigation methods and authorities are generally ill-equipped to deal with cybercrime. The investigators are no longer dealing purely with tangible physical items situated on premises, but are required to investigate crimes

[62] E. Casey, (2011), *Digital Evidence and Computer Crime*, *Forensic Science Computers and the Internet,* Elsevier, 132 (2011).
[63] D. Colarusso, Heads in the Cloud, a Coming Storm: The Interplay of Cloud Computing, Encryption, and the Fifth Amendment's Protection Against Self-Incrimination', 17 *Boston University Journal of Science & Technology Law*, 69, 92-93 (2011).
[64] The Council of Europe's Explanatory Report to the Cybercrime Convention, (Jan. 23, 2025, 03:30 PM) https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf.
[65] Budapest Convention on Cybercrime, art. 19.
[66] *Ibid*.
[67] *Ibid*.
[68] R. Proust, *International co-operation: A Commonwealth perspective*, 16(3) *SA Journal of Criminal Justice* 295 (2003).

perpetrated through highly sophisticated technology, and sometimes through borderless information networks.[69]

Search-and-seizure investigations are coercive measures which infringe upon an individual's right to privacy and associated fundamental human rights. On the basis of the fact that the central doctrine of international law maintains that jurisdiction is strictly territorial in nature, an effective domestic legal mechanism is critically imperative.[70]

E. Anonymity & Attribution

Unlike most traditional crimes, cybercrimes can be undertaken on a large scale and one offender may be linked to a vast number of smaller crimes (for example, a botnet which is able to send out masses of phishing emails). In most of these situations the offender would be perceived as largely anonymous by the victim. Data collection and recording in this area will therefore face particular challenges in linking together seemingly isolated incidents.[71]

1. Reasons causing Anonymity-

The common techniques which are being used by the cybercriminals to increase their anonymity include-

a. *Different Internet Access Points-*

When an individual uses different internet access points (as opposed to typical, household internet connections), it requires (significantly) more effort on the part of law enforcement officials to trace back an IP address.[72] Individuals can make use of- (a) a WiFi connection of another person, (b) a computer at a cybercafé, and (c) publicly available internet connections (called 'hotspots') at airports, restaurants, or hotels, in order to access the Internet.[73] Following of the digital leads allocated to these access points do not lead the law enforcement officials directly to the IP Address of the suspect, making it more difficult for them to identify the culprit.

b. Anonymising services

---

[69] Vinesh M Basdeo, Moses Montesh and Bernard Khotsu Lekubu, *Search for and Seizure of Evidence in Cyber Environments: A Law- Enforcement Dilemma in South African Criminal Procedure*, 1 (1) Journal of Law, Society and Development 48, 62 (Jan.15, 2025) https://doi.org/10.25159/2520-9515/874.
[70] *Id* at 59.
[71] Dr. Mike McGuire and Samantha Dowling, Cybercrime: A review of Evidence (Feb. 27, 2025 at 6:25 PM) https://assets.publishing.service.gov.uk/media/5a7caa0340f0b65b3de0a624/horr75-chap4.pdf.
[72] J.J. Oerlemans, *Investigating Cybercrime, pg. 37* (Aug. 25, 2025, 5:25 PM) *https://scholarlypublications.universiteitleiden.nl/handle/1887/44879*
[73] UNODC 2012.

There are many anonymising services available on the Internet that make it harder for law enforcement officials to track down suspects based on their IP address.[74]

The following three services are briefly discussed to illustrate how anonymising services challenge law enforcement officials in gathering evidence:[75]

i. Proxy services:

Proxy services are services that send network traffic through an intermediary computer; such computers are called 'proxy servers'. A proxy server functions as a gateway. Proxy services strip away the originating IP address.[76] The public IP address of the network connection that a suspect uses is changed to the proxy server's address.[77]

ii. VPN (Virtual Private Network) services-

Virtual Private Network services (VPN services) are services that route traffic through an intermediary server, thereby changing the originating (public) IP address of an internet user. VPN services encrypt the internet traffic in transit.[78]

Proxy-service providers and VPN-service providers provide more anonymity to internet users, because it requires more effort from law enforcement officials to trace an IP address back to the computer user. In essence, intermediary computers are an additional link in the chain.[79]

iii. Tor

Tor is a system designed to anonymise network traffic.[80] It *encrypts* network traffic, and it *routes* traffic through relays on its network. Internet traffic goes 'one hop at a time' through relays.[81] Each relay only knows which relay sent the data to it (the last sender) and the next relay through which the data will be routed (first addressee). No individual relay knows the complete path that the network traffic has taken. The Tor system makes sure that traffic

[74] UNODC 2013, p. 143, available at https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf accessed on 23rd September 2024.
[75] It is important to note that these three anonymising services are not the only services that provide a degree of anonymity online. For example, Freenet is publicly available soft-ware that enables users to anonymously share files and visit websites (see Clarke et al. 2001, and Clarke et al. 2010). In addition, anonymity networks that are still in development – in particular the Invisible Internet Project ('I2P') – may prove to be popular in the near future (cf. Ciancaglini et al. 2013, p. 18).
[76] These can be commercially available proxy services, but hacked computers can also act as a gateway for the network traffic of criminals (see Bernaards, Monsma & Zinn 2012, p. 61)
[77] Hagy 2007, p. 51-52
[78] Investigating Cybercrime, pg. 39, accessed on 23rd September 2024
[79] Internet users can even send network traffic from one proxy to another proxy server or VPN server to create additional links in the chain, e.g., creating a series of obstacles in a criminal investigation. However, the technique may delay network traffic and can create several points of weakness in the ICT infrastructure (cf. Van den Eshof et al. 2002, p. 34-35).
[80] Tor is an abbreviation for 'The Onion Routing'.
[81] Tor relays are also referred to as 'routers' or 'nodes'.

 [ISSN 2581-5369]

analysis techniques cannot establish a link to the connection's source and destination.[82] Apart from providing the means to hide the originating IP address, the Tor system also allows individuals to access 'hidden services' (websites or online services that are only accessible to computers that make use of the Tor system) on the Internet. The combination of those websites and services that are publicly accessible and that also hide the IP addresses of the servers that run them are referred to as the 'Dark Web'.[83]

V. SUGGESTION AND CONCLUSION

Development of Balanced Procedural Instruments that enable competent authorities to investigate and adjudicate cybercrime and protect rights of suspect-

1. The procedural instruments should not interfere with the internationally as well as regionally accepted fundamental rights of the suspect.
2. Reporting mechanisms such as 'panic button' apps in mobile devices or websites could play an instrumental role in reporting abuse suffered by the internet users.
3. The law enforcement officials need to build trust relationships with the stakeholders that sensitive crimes would be investigated tactfully and discreetly to encourage reporting of sensitive crimes.
4. Provision should be made to enable the competent authorities to expedite the preservation of computer data.
5. There should be a provision enabling competent authorities to use specific search and seizure instruments related to digital evidence and computer technology.
6. There should be a provision enabling competent authorities to order the lawful collection of traffic data and the lawful interception of content data.
7. There should be a provision enabling competent authorities to make use of sophisticated investigation instruments such as the use of key-loggers and remote forensic software, especially in cases of serious crimes, to collect passwords used by a suspect of such crime or identify the connection used by a suspect.

[82] This description of Tor is derived from the article 'Tor: overview' from the website of the Tor project. (Sept. 23, 2024, 11:30 AM) https://www.torproject.org/about/overview.html.en.

[83] Andy Greenberg, *Hacker Lexicon: What Is the Dark Web?*, Wired. (Nov. 20, 2024, 12:20 PM) http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/.

 [ISSN 2581-5369]

8. To test the reliability of the evidence, the court must conduct a meaningful analysis of the computer system in which the input procedures, database and processing program should be tested separately for accuracy.
9. Judicial notice must be taken of the reliability of the computerized machines. There must be a shift in the burden of proof to show the unreliability of a computer system. Greater emphasis must be laid on the accuracy of data input and software as foundational requirements because bugs in data input can lead to massive error and insurmountable problems.

Framework to regulate the Responsibility of Internet Service Providers-

1. Criminal liability should be fixed on the *access/service provider* if it fails to initiate steps to prevent transmission, modify the information, inform the authorities regarding offences which were committed by the users of their service.
2. Further there must be a criminal liability affixed on the *Caching Provider* for automatic, intermediate and temporary storage of information.
3. The framework should also limit the criminal responsibility of the *Hosting Provider*, if he has no knowledge about the existence of illegal data or he illegally removes them on obtaining such knowledge, without prior informing the respective authorities.

Capacity Building/ Incorporation of Technological Advancements-

1. Use of Artificial Intelligence
    a. Deep learning, machine learning, and other AI-based tools may all be used to find patterns, abnormalities, and other signs of cyberattacks.
    b. AI can help law enforcement agencies locate and follow cybercriminals, analyse enormous amounts of information to find suspicious activity, and forecast and stop potential assaults.
2. Cyber Forensics-

Live data forensic expertise and capabilities must be improved to take into consideration factors such as existence of encrypted containers in the offenders' devices and the use of remote storages by them.

3. Cryptography-

To have any probative value, digital evidence must be validated. The contents of a number of disks or storage devices are invariably copied and to prove that the digital evidence is not

 [ISSN 2581-5369]

altered, necessary checks and balances must be put in place. Electronic fingerprint can be used to prove the integrity of the digital evidence, that it is not altered since it was copied.

Spreading Awareness

1. The law enforcement officials should increase their presence online to address the issue of lack of visibility of authorities in cyberspace so that the confidence of public in security of the internet may increase and deter the criminals.
2. There must be regular use of available communication platforms including social media by the law enforcement officials in order to highlight the latest threats and scams to the general internet users. This will help in quick dissemination of information and strengthening of community relations.

Legal Co-operation among States at International Level/Transnational Cooperation-

States must establish and designate agencies to deal with transnational issues, and to cooperate with counterparts throughout the world. The framework must include creation of a designated 24/7 point of contact for request. Use of expedited means of communication (email, fax, etc.) should be promoted.

Better collaboration between Decision Makers and Technology Experts-

A prudent approach must be adopted by the government and the courts by setting up a team of digital evidence specialists who would assist the courts and specifically determine the authenticity of the electronic evidence. Skilled civilians/ experts should be granted same search and seizure powers as the police officers, whom they accompany during the investigation of cybercrime. Currently, they only act as assistants to the police personnel.

*****

 [ISSN 2581-5369]